UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: GOOGLE INC. GMAIL LITIGATION THIS DOCUMENT RELATES TO: **ALL ACTIONS**	Case No.: 13-MD-02430-LHK ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS [REDACTED]

In this consolidated multi-district litigation, Plaintiffs Keith Dunbar, Brad Scott, Todd Harrington, Matthew Knowles, A.K. (next of friend to Minor J.K.), Brent Matthew Scott, Kristen Brinkman, Robert Fread, and Rafael Carrillo, individually and on behalf of those similarly situated (collectively, "Plaintiffs"), allege that Defendant Google, Inc., has violated state and federal anti-wiretapping laws in its operation of Gmail, an email service. *See* ECF No. 38-2. Before the Court is Google's Motion to Dismiss Plaintiffs' Consolidated Complaint. *See* ECF No. 44. For the reasons stated below, the Court DENIES in part and GRANTS in part Google's Motion to Dismiss with leave to amend.

I. BACKGROUND

A. Factual Allegations

Plaintiffs challenge Google's operation of Gmail under state and federal anti-wiretapping laws. The Consolidated Complaint seeks damages on behalf of a number of classes of Gmail users and non-Gmail users for Google's interception of emails over a period of several years. All the class periods span from two years prior to the filing of the actions to the date of class certification, if any. Because the first of these consolidated actions was filed in 2010, the Consolidated Complaint taken as a whole challenges the operation of Gmail from 2008 to the present.

1. Google's Processing of Emails

Google's processing of emails to and from its users has evolved over the putative class periods. Plaintiffs allege, however, that in all iterations of Google's email routing processes since 2008, Google has intercepted, read, and acquired the content of emails that were sent or received by Gmail users while the emails were in transit. Plaintiffs allege that before [redacted] 20[redacted], a Gmail device intercepted, read, and acquired the content of each email for the purposes of sending an advertisement relevant to that email communication to the recipient, sender, or both. ECF No. 38-2 ¶¶ 26–27, 33. According to the Consolidated Complaint, this interception and reading of the email was separate from Google's other processes, including spam and virus filtering. *Id.* ¶ 5.

After [redacted] 20[redacted], Plaintiffs allege that Google continued to intercept, read, and acquire content from emails that were in transit even as Google changed the way it transmits emails. Plaintiffs allege that after [redacted] 20[redacted], Google continued to intercept, read, and acquire content from emails to provide targeted advertising. *Id.* ¶¶ 62–63. Moreover, Plaintiffs allege that post-[redacted] 20[redacted], targeted advertising was not the sole purpose of the interception. Rather, during this time period, Plaintiffs allege that a number of Google devices intercepted the emails, read and collected content as well as affiliated data, and [redacted] these emails and data. *Id.* ¶¶ 47–56. Plaintiffs further allege that Google used these [redacted] data to create user profiles and models. *Id.* ¶¶ 74–79. Google then allegedly used the emails, affiliated data, and user profiles to serve their

profit interests that were unrelated to providing email services to particular users. *Id.* ¶¶ 97–98. Accordingly, Plaintiffs allege that Google has, since 20[redacted], intercepted emails for the dual purposes of providing advertisements and creating user profiles to advance Google's profit interests.

2. Types of Gmail Services

Gmail implicates several different, but related, systems of email delivery, three of which are at issue here. The first is a free service, which allows any user to register for an account with Google to use Gmail. *Id.* ¶ 99. This system is supported by advertisements, though users can opt-out of such advertising or access Gmail accounts in ways that do not generate advertising, such as accessing email on a smartphone. *Id.* ¶ 70.

The second is Google's operation of email on behalf of Internet Service Providers ("ISPs"). *Id.* ¶ 100. Google, through its Google Apps Partner program, enters into contracts with ISPs, such as Cable One, to provide an email service branded by the ISP. *Id.* The ISP's customers can register for email addresses from their ISP (such as "@mycableone.com"), but their email is nevertheless powered by Google through Gmail.

Third, Google operates Google Apps for Education, through which Google provides email on behalf of educational organizations for students, faculty, staff, and alumni. *Id.* ¶ 101. These users receive "@name.institution.edu" email addresses, but their accounts are also powered by Google using Gmail. *Id.* Universities that are part of Google Apps for Education require their students to use the Gmail-provided service. *Id.*

Google Apps users, whether through the educational program or the partner program, do not receive content-based ads but can opt in to receiving such advertising. Google processes emails sent and received from all Gmail users,[1] including Google Apps users, in the same way

[1] In this Order, the Court uses "Gmail users" to refer to individuals who send or receive emails using the free Gmail service or Google apps. "Non-Gmail users" refers to email users who do not themselves use Gmail (through the free service or Google Apps). "Google Apps users" refers to the subset of Gmail users who access Gmail through either the Google Apps Partner Program or Google Apps for Education.

except that emails of users who do not receive advertisements are not processed through Google's advertising infrastructure, which attaches targeted advertisements to emails. *Id.* ¶¶ 57, 72–73. This means that users who do not receive advertisements would not have been subject to the pre-[redacted] 20[redacted] interceptions, as during that period, interceptions were for the sole purpose of attaching targeted advertisements to emails. After [redacted] 20[redacted], Google separated its interception of emails for targeted advertising from its interception of emails for creating user profiles. *Id.* ¶ 72. As a result, after [redacted] 20[redacted], emails to and from users who did not receive advertisements are nevertheless intercepted to create user profiles. *Id.* ¶¶ 73, 85. Accordingly, these post-[redacted] 20[redacted] interceptions impacted all Gmail and Google Apps users, regardless of whether they received advertisements.

3. Google's Agreements with Users

The operation of the Gmail service implicates several legal agreements. Gmail users were required to agree to one of two sets of Terms of Service during the class periods. The first Terms of Service was in effect from April 16, 2007, to March 1, 2012, and the second has been in effect since March 1, 2012. *Id.* ¶ 102. The 2007 Terms of Service stated that:

> Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service. For some Services, Google may provide tools to filter out explicit sexual content. These tools include the SafeSearch preference settings . . . . In addition, there are commercially available services and software to limit access to material that you may find objectionable.

Id. ¶ 104. A subsequent section of the 2007 Terms of Service provided that "[s]ome of the Services are supported by advertising revenue and may display advertisements and promotions" and that "[t]hese advertisements may be content-based to the content information stored on the Services, queries made through the Service or other information." *Id.* ¶¶ 107–08.

The 2012 Terms of Service deleted the above language and stated that users "give Google (and those [Google] work[s] with) a worldwide license to use . . ., create derivative works (such as

those resulting from translations, adaptations or other changes we make so that your content works better with our Services), . . . and distribute such content." *See* ECF No. 46-6 at 3.

Both Terms of Service reference Google's Privacy Policies, which have been amended three times thus far during the putative class periods. *See* ECF Nos. 46-7, 46-8, 46-9, 46-10. These Policies, which were largely similar, stated that Google could collect information that users provided to Google, cookies, log information, user communications to Google, information that users provide to affiliated sites, and the links that a user follows. *See* ECF No. 46-7. The Policies listed Google's provision of "services to users, including the display of customized content and advertising" as one of the reasons for the collection of this information. *Id.*

Google also had in place Legal Notices, which stated that "Google does not claim any ownership in any of the content, including any text, data, information, images, photographs, music, sound, video, or other material, that [users] upload, transmit or store in [their] Gmail account." ECF No. 38-2 ¶ 118. The Notices further stated that Google "will not use any of [users'] content for any purpose except to provide [users] with the service." *Id.* ¶ 121.

In addition, Google entered into contractual agreements with ISPs and educational institutions as part of its Google Apps Partner and Google Apps for Education programs. These agreements require Google to "protect against unauthorized access to or use of Customer data." *Id.* ¶¶ 137, 161. In turn, "Customer data" is defined as "data, including email, provided, generated, transmitted, or displayed via the Services by Customers or End Users." *Id.* ¶¶ 138, 162. Further, the Terms of Service applicable to Google Apps Cable One users states that "Google may access, preserve, and disclose your account information and any Content associated with that account if required to do so by law or in a good faith belief that such access preservation or disclosure is reasonably necessary" to satisfy applicable law, enforce the Terms of Service, detect or prevent fraud, or protect against imminent harm to the rights of Google, its users, or the public. ECF No. 46-2 at 2–3.

Importantly, Plaintiffs who are not Gmail or Google Apps users are not subject to any of Google's express agreements. Because non-Gmail users exchange emails with Gmail users, however, their communications are nevertheless subject to the alleged interceptions at issue in this case.

4. Relief Sought and Class Allegations

Plaintiffs bring these cases alleging that Google, in the operation of its Gmail system, violated federal and state anti-wiretapping laws. ECF No. 38-2 ¶ 216 (federal law), ¶ 288 (California law), ¶ 328 (Maryland law), ¶ 349 (Florida law), ¶ 370 (Pennsylvania law). Plaintiffs seek the certification of several classes, preliminary and permanent injunctive relief, declaratory relief, statutory damages, punitive damages, and attorneys' fees. Plaintiffs seek relief on behalf of the following classes, all of which have a class period starting two years before the relevant complaint was filed and running through the date of class certification, if any:

(1) all Cable One users who sent a message to a Gmail user and received a reply or received an email;

(2) all Google Apps for Education users who have sent a message to a Gmail user and received a reply or received an email;

(3) all U.S. citizen non-Gmail users (except California residents) who have sent a message to a Gmail user and received a reply or received an email from a Gmail user;

(4) all U.S. citizen non-Gmail users who have sent a message to a Gmail user and received a reply or received an email from a Gmail user;

(5) all Pennsylvania non-Gmail users who have sent a message to a Gmail user and received a reply or received an email from a Gmail user;

(6) all Florida non-Gmail users who have sent a message to a Gmail user and received a reply or received an email from a Gmail user;

(7) all Maryland non-Gmail users who have sent a message to a Gmail user and received a reply or received an email from a Gmail user; and

(8) all Gmail users who were under the age of majority and who used Gmail to send an email to or received an email from a non-Gmail user or a Gmail user under the age of majority. *Id.* ¶¶ 388–92.

B. Procedural History

This case is a consolidated multi-district litigation involving seven individual and class action lawsuits. *See* ECF No. 38-2. The first of these consolidated actions was filed on November 17, 2010, and transferred from the Eastern District of Texas to the Northern District of California on June 27, 2012. *See Dunbar v. Google, Inc.*, 12-CV-03305 (N.D. Cal.); ECF No. 179. Five other actions involving substantially similar allegations against Google followed in this District and throughout the country. *See Scott, et al. v. Google, Inc.*, No. 12-CV-03413 (N.D. Cal.); *Scott v. Google, Inc.*, No. 12-CV-00614 (N.D. Fla.); *A.K. v. Google, Inc.*, No. 12-CV-01179 (S.D. Ill.); *Knowles v. Google, Inc.*, 12-CV-02022 (D. Md.); *Brinkman v. Google, Inc.*, 12-CV-06699 (E.D. Pa.). On April 1, 2013, the Judicial Panel on Multidistrict Litigation issued a Transfer Order, centralizing these six actions in the Northern District of California before the undersigned judge. *See* ECF No. 1. On May 6, 2013, this Court related a seventh action, *Fread v. Google, Inc.*, 13-CV-01961 (N.D. Cal.), as part of this multi-district litigation. *See* ECF No. 29.

Plaintiffs filed an Administrative Motion to file their Consolidated Complaint under seal on May 16, 2013.[2] *See* ECF No. 38. The Complaint contained five claims alleging violations of: (1) the Wiretap Act, as amended by the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510, *et seq.*; (2) the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630, *et seq.*; (3) the Maryland Courts and Judicial Proceedings Code Ann. §§ 10-402, *et seq.*; (4) Florida Statute §§ 934.03, *et seq.*; and (5) 18 Pa. Const. Stat. §§ 5701, *et seq.* *See* ECF No. 38-2.

Google filed a Motion to Dismiss the Consolidated Complaint on June 13, 2013. *See* ECF No. 44. On the same day, Google filed two declarations and a request for judicial notice in support

[2] The Court resolves this Administrative Motion through a separate order.

of its Motion. *See* ECF Nos. 45–47. Plaintiffs filed an opposition to Google's request for judicial notice and separate objections to Google's declarations on July 11, 2013. *See* ECF Nos. 49–50. Google filed a reply in support of its request for judicial notice and Motion to Strike Plaintiffs' objections to Google's declarations on July 29, 2013. ECF No. 58.

Plaintiffs filed their opposition to Google's Motion to Dismiss on July 11, 2013. *See* ECF No. 53. That same day, Plaintiffs filed a request for judicial notice in support of their opposition. *See* ECF No. 51. Google filed a reply along with a declaration in support of the reply on July 29, 2013. *See* ECF No. 56–57. This Court held a hearing on the Motion to Dismiss on September 5, 2013. *See* ECF No. 64.

II. LEGAL STANDARDS

A. Motion to Dismiss

Pursuant to Federal Rule of Civil Procedure 12(b)(6), a defendant may move to dismiss an action for failure to allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal citations omitted). For purposes of ruling on a Rule 12(b)(6) motion, the Court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the non-moving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

However, a court need not accept as true allegations contradicted by judicially noticeable facts, *Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and a "court may look beyond the plaintiff's complaint to matters of public record" without converting the Rule 12(b)(6) motion into a motion for summary judgment, *Shaw v. Hahn*, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995). A court is also not required to "'assume the truth of legal conclusions merely because they are cast in

the form of factual allegations.'" *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam) (quoting *W. Min. Council v. Watt*, 643 F.2d 618, 624 (9th Cir. 1981)). Mere "conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss." *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004); *accord Iqbal*, 556 U.S. at 678. Furthermore, "a plaintiff may plead herself out of court" if she "plead[s] facts which establish that [s]he cannot prevail on h[er] . . . claim." *Weisbuch v. Cnty. of L.A.*, 119 F.3d 778, 783 n.1 (9th Cir. 1997) (internal quotation marks and citation omitted).

B. Request for Judicial Notice

The Court generally may not look beyond the four corners of a complaint in ruling on a Rule 12(b)(6) motion, with the exception of documents incorporated into the complaint by reference, and any relevant matters subject to judicial notice. *See Swartz v. KPMG LLP*, 476 F.3d 756, 763 (9th Cir. 2007); *Lee v. City of Los Angeles*, 250 F.3d 668, 688–89 (9th Cir. 2001). Under the doctrine of incorporation by reference, the Court may consider on a Rule 12(b)(6) motion not only documents attached to the complaint, but also documents whose contents are alleged in the complaint, provided the complaint "necessarily relies" on the documents or contents thereof, the document's authenticity is uncontested, and the document's relevance is uncontested. *Coto Settlement v. Eisenberg*, 593 F.3d 1031, 1038 (9th Cir. 2010); *see Lee*, 250 F.3d at 688–89. The purpose of this rule is to "prevent plaintiffs from surviving a Rule 12(b)(6) motion by deliberately omitting documents upon which their claims are based." *Swartz*, 476 F.3d at 763 (internal quotation marks omitted).

The Court also may take judicial notice of matters that are either (1) generally known within the trial court's territorial jurisdiction or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. Fed. R. Evid. 201(b). Proper subjects of judicial notice when ruling on a motion to dismiss include legislative history reports, *see Anderson v. Holder*, 673 F.3d 1089, 1094, n.1 (9th Cir. 2012); court documents already in the public record and documents filed in other courts, *see Holder v. Holder*, 305 F.3d 854, 866 (9th

Cir. 2002); and publically accessible websites, *see Caldwell v. Caldwell*, 2006 WL 618511, at *4 (N.D. Cal. Mar. 13, 2006); *Wible v. Aetna Life Ins. Co.*, 375 F. Supp. 2d 956, 965–66 (C.D. Cal. 2005).

C. Leave to Amend

If the Court determines that the complaint should be dismissed, it must then decide whether to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend "shall be freely given when justice so requires," bearing in mind "the underlying purpose of Rule 15 . . . [is] to facilitate decision on the merits, rather than on the pleadings or technicalities." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (internal quotation marks and citation omitted). Nonetheless, a court "may exercise its discretion to deny leave to amend due to 'undue delay, bad faith or dilatory motive on part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party . . ., [and] futility of amendment.'" *Carvalho v. Equifax Info. Servs., LLC*, 629 F.3d 876, 892–93 (9th Cir. 2010) (quoting *Foman v. Davis*, 371 U.S. 178, 182 (1962)) (alterations in original).

III. REQUESTS FOR JUDICIAL NOTICE

In support of their opposition to Google's Motion to Dismiss, Plaintiffs request the Court take judicial notice of (A) a declaration and a motion filed in *Sheppard v. Google, Inc., et al*, 12-CV-4022 (W.D. Ark.); (B) an excerpt of a November 30, 1985 Senate Judiciary Committee hearing regarding the ECPA; (C) an April 29, 1968 Senate Report; and (D) an order on Google's motion to dismiss in *Marquis v. Google, Inc.*, No. 11-2808, in the Superior Court of Suffolk County, Commonwealth of Massachusetts. *See* ECF No. 51. Plaintiffs' Exhibits B and C are legislative history reports, and Plaintiffs' Exhibits A and D are documents filed in other courts, already part of the public record. *See Anderson*, 673 F.3d at 1094, n.1; *Holder*, 305 F.3d at 866. Google does not oppose any of these requests. The Court takes judicial notice of all four.

Google requests that the Court take judicial notice of (A) a copy of Google's Terms of Service applicable to Google Apps services provided through Cable One, Inc.; (B) a copy of the

Google Apps Education Edition Agreement between Google and the University of Hawaii; (C) a copy of the Google Apps Education Edition Agreement between Google and the University of the Pacific; (D) copies of Google's Terms of Service dated April 16, 2007 and March 1, 2012; (E) copies of Google's Privacy Policies dated August 7, 2008, March 11, 2009, October 3, 2010, and March 1, 2012; (F) a copy of the Yahoo! Mail Privacy Policy from June 2013; (G) an excerpt of an October 17, 1986 Senate Report regarding the ECPA; (H) a copy of a May 9, 1995 California Senate Judiciary Committee analysis; and (I) a copy of an April 13, 2010 California Senate Public Safety Committee analysis. *See* ECF No. 47. Plaintiffs oppose the request for judicial notice with respect to items F, G, H, and I. *See* ECF No. 49.

The Court takes judicial notice of items A, B, C, D, and E as requested by Google and to which Plaintiffs do not object because Plaintiffs rely upon and reference these documents in the Complaint. *See* ECF No. 38-2 ¶¶ 102, 144, 185–86, 189, 227–28, 237–38; *Coto*, 593 F.3d at 1038. The Court further takes judicial notice of items H and I because Plaintiffs "do[] not contest that these are readily available public documents or challenge their authenticity." *Zephyr v. Saxon Mortg. Servs., Inc.*, 873 F. Supp. 2d 1223, 1226 (E.D. Cal. 2012). The Court takes judicial notice of item G because it is a legislative history report for the statute at the heart of Plaintiffs' principal claim. *See id.; Anderson*, 673 F.3d at 1094, n.1. Finally, the Court denies Google's request for judicial notice of item F, the Yahoo! Mail Privacy Policy. The Policy is not a document "on which the Complaint necessarily relies nor . . . whose relevance and authenticity are uncontested" because Plaintiffs contend that the effective dates of the Yahoo! Privacy Policy are unknown. *See* ECF No. 49 at 2–3; *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 795 (N.D. Cal. 2011).

Plaintiffs further raise objections to various paragraphs in the declarations supporting Google's Motion to Dismiss and to the requests for judicial notice with respect to some of the exhibits attached to the declarations. *See* ECF No. 50. The Court strikes these objections pursuant to Civil Local Rule 7-3(a). The Rule requires that any evidentiary objections to a motion be contained within the opposition to the motion itself, but Plaintiffs filed their objections separately

from their opposition. *See Apple, Inc. v. Samsung Elecs. Co., Ltd.*, 2011 WL 7036077, at *3 (N.D. Cal. Dec. 2, 2011).

IV. MOTION TO DISMISS

A. The Wiretap Act

The Wiretap Act, as amended by the ECPA, generally prohibits the interception of "wire, oral, or electronic communications." 18 U.S.C. § 2511(1); *see also Joffe v. Google, Inc.*, No. 11-17483, 2013 WL 4793247, at *3 (9th Cir. Sept. 10, 2013). More specifically, the Wiretap Act provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a); *see id.* § 2520 (providing a private right of action for violations of § 2511). The Act further defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4).

Plaintiffs contend that Google violated the Wiretap Act in its operation of the Gmail system by intentionally intercepting the content of emails that were in transit to create profiles of Gmail users and to provide targeted advertising. Google contends that Plaintiffs have not stated a claim with respect to the Wiretap Act for two reasons. First, Google contends that there was no interception because there was no "device." Specifically, Google argues that its reading of any emails would fall within the "ordinary course of business" exception to the definition of device. ECF No. 44 at 6–13. Under that exception, "any telephone or telegraph instrument, equipment or facility, or any component thereof . . . being used by a provider of wire or electronic communication service in the ordinary course of its business" is not a "device," and the use of such an instrument accordingly falls outside of the definition of "intercept." 18 U.S.C. § 2510(5)(a)(ii). Second, Google contends that all Plaintiffs have consented to any interception. ECF No. 44 at 13–20. Under the statute, it is not unlawful "to intercept a wire, oral, or electronic communication . . .

where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d).

1. "Ordinary Course of Business" Exception

Google first contends that it did not engage in an interception because its reading of users' emails occurred in the ordinary course of its business. ECF No. 44 at 6–13. Conversely, Plaintiffs contend that the ordinary course of business exception is narrow and applies only when an electronic communication service provider's actions are "necessary for the routing, termination, or management of the message." *See* ECF No. 53 at 7. The Court finds that the ordinary course of business exception is narrow. The exception offers protection from liability only where an electronic communication service provider's interception facilitates the transmission of the communication at issue or is incidental to the transmission of such communication. Specifically, the exception would apply here only if the alleged interceptions were an instrumental part of the transmission of email. Plaintiffs have alleged, however, that Google's interception is not an instrumental component of Google's operation of a functioning email system. ECF No. 38-2 ¶ 97. In fact, Google's alleged interception of email content is primarily used to create user profiles and to provide targeted advertising — neither of which is related to the transmission of emails. *See id.* ¶¶ 26–27, 33, 57, 65, 84, 95. The Court further finds that Plaintiffs' allegations that Google violated Google's own agreements and internal policies with regard to privacy also preclude application of the ordinary course of business exception.

The plain language of the Wiretap Act, 18 U.S.C. § 2510(5)(a), exempts from the definition of "device":

> any telephone or telegraph instrument, equipment or facility, or any component thereof,
>
> (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

> (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

This section includes two "ordinary course of business" exceptions. The first, under subsection (a)(i), is for users or subscribers of electronic communication services, while the second, subsection (a)(ii), applies to the providers of electronic communication services themselves. This case implicates the latter, as Google provides the electronic communication service at issue here, Gmail.

The Sixth Circuit has found that the text of "[t]he two exceptions [is] not altogether clear." *Adams v. City of Battle Creek*, 250 F.3d 980, 982 (6th Cir. 2001). There is no dispute that Google's interception of Plaintiffs' emails and subsequent use of the information to create user profiles or to provide targeted advertising advanced Google's business interests. But this does not end the inquiry. The Court must give effect to the word "ordinary," which limits "course of business" under both exceptions. The presence of the modifier "ordinary" must mean that not everything Google does in the course of its business would fall within the exception. The task the Court faces at this stage is to determine whether Plaintiffs have adequately alleged that the purported interceptions were not an "ordinary" part of Google's business.

In the context of section 2510(5)(a)(i), courts have held, consistent with the textual limitation that "ordinary" imposes on "course of business," that not everything that a company may want to do falls within the "ordinary course of business" exception. *See e.g., Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983) ("The phrase 'in the ordinary course of business' cannot be expanded to mean anything that interests a company."). Rather, the business reasons must be "legitimate." *See Arias v. Mut. Cent. Alarm Serv., Inc.*, 202 F.3d 553, 559 (2d Cir. 2000); *see also Berry v. Funk*, 146 F.3d 1003, 1009 (D.C. Cir. 1998) (finding that actions are in the ordinary course of business if they are "justified by a valid business purpose" or "shown to be undertaken normally").

This limitation, applied to electronic communication service providers in the context of section 2510(5)(a)(ii), means that the electronic communication service provider engaged in the alleged interception must demonstrate the interception facilitated the communication service or was incidental to the functioning of the provided communication service. For example, in *Kirch v. Embarq Management Co.*, 702 F.3d 1245 (10th Cir. 2012), which Google cites, ECF No. 44 at 9, the Tenth Circuit affirmed a grant of summary judgment in favor of Embarq, an ISP, where Embarq had intercepted only data incidental to its provision of the internet service. In that case, Embarq had granted a third party, NebuAd, permission to conduct a technology test by acquiring information about Embarq's users so that NebuAd could provide targeted advertising to those users. 702 F.3d at 1247. The Tenth Circuit held that Embarq had not violated the ECPA because the ISP could not be liable for NebuAd's interceptions. *Id.* at 1249. Further, Embarq itself did not review any of the raw data that NebuAd collected. *Id.* at 1250. Rather, Embarq had no more access than it otherwise would have had as an ISP. *Id.* Embarq's ordinary course of business as an ISP necessarily required that it would have access to data that was transmitted over its equipment. *Id.* at 1249. The relationship between Embarq and NebuAd's technology test did not expand the universe of data to which Embarq had access beyond the data Embarq could access in its provision of internet services. *Id.* at 1250. Accordingly, Embarq's actions fell within its ordinary course of business. Unlike this case, the only information to which Embarq had access was collected by Embarq's devices that provided internet services. *Id*. In contrast, here, Plaintiffs allege that there are separate devices — aside from the devices related to delivery of email — that intercept users' emails. ECF No. 38-2 ¶ 259(e). Considered practically, Google is more akin to NebuAd, which intercepted data for the purpose of providing targeted advertising — a purpose separate and apart from Embarq's provision of internet service. *Cf. Kirch*, 702 F.3d at 1248. However, because NebuAd settled with the Plaintiffs in *Kirch*, the Tenth Circuit's opinion does not deal with NebuAd's liability. *Id.* at 1248 n. 2, 1249 ("[W]e need not address whether NebuAd intercepted any of the Kirches' electronic communications."). The Court therefore finds that *Kirch*'s

discussion of Embarq's liability cuts in favor of a narrow reading of the section 2510(5)(a)(ii) exception and that *Kirch* stands only for the narrow proposition that interceptions incidental to the provision of the alleged interceptor's internet service fall within the "ordinary course of business" exception.

Hall v. Earthlink Network, Inc., 396 F.3d 500 (2d Cir. 2005), which also addresses the section 2510(5)(a)(ii) exception, further suggests that this Court should narrowly read the "ordinary course of business" exception. There, the Second Circuit affirmed a grant of summary judgment and concluded that Earthlink did not violate the ECPA when Earthlink continued to receive and store emails sent to an address that had been closed. The Second Circuit found that the plaintiff in that case did not present any evidence that Earthlink's continued receipt of emails was outside its ordinary course of business. *Id.* at 505. The Court noted that Earthlink presented testimony that Earthlink routinely continued to receive and store emails after an account was canceled and more critically that Earthlink "did not have the ability to bounce e-mail back to senders after the termination of an account." *Id.* Accordingly, in *Hall*, the email provider's alleged interceptions were a necessary part of its ability to provide email services. In the instant case, by contrast, Plaintiffs have alleged that Google could operate its Gmail system without reading the emails for the purposes of targeted advertising or the creation of user profiles. ECF No. 38-2 ¶ 97. Therefore, unlike *Earthlink*, the alleged interception in the instant case is not incidental to the operation of the service.[3]

[3] The Court finds that *In re Google, Inc. Privacy Policy Litigation*, 2012 WL 6738343 (N.D. Cal. Dec. 28, 2012), does not suggest a broader reading of the exception. Google relies on that case for the proposition that as long as Google is using its own devices, Google cannot be intercepting users' information. ECF No. 44 at 9–10. Yet, the court in *Privacy Policy* explicitly noted that the use of the device must be in the ordinary course of business. *See In re Google, Inc. Privacy Policy Litigation*, 2012 WL 6738343 at *5–6. Further, unlike that case, the alleged interception in the instant case occurred while the email was in transit, rather than when the material was already in possession of the intended recipient. *See id.* at *6 (dismissing plaintiffs' cause of action on the basis that they "utterly fail . . . to cite any authority that supports either the notion that a provider can intercept information already in its possession by violating limitations imposed by a privacy policy or the inescapably plain language of the Wiretap Act that excludes from the definition of a 'device' a provider's own equipment used in the ordinary course of business."). The difference

In addition to the text and the case law, the statutory scheme and legislative history also weigh in favor of a narrow reading of the section 2510(5)(a)(ii) exception. Specifically, a separate exception to the Wiretap Act related to electronic service providers states that:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring *except for mechanical or service quality control checks*.

18 U.S.C. § 2511(2)(a)(i) (emphasis added). The statute explicitly limits the use of service observing or random monitoring by electronic communication service providers to mechanical and service quality control checks. *Id.* Accordingly, the statutory scheme suggests that Congress did not intend to allow electronic communication service providers unlimited leeway to engage in any interception that would benefit their business models, as Google contends. In fact, this statutory provision would be superfluous if the ordinary course of business exception were as broad as Google suggests. *See Duncan v. Walker*, 533 U.S. 167, 174 (2001) (stating that in statutory interpretation, courts should "give effect, if possible, to every clause and word of a statute").

The legislative history of section 2511(2)(a)(i), which Google cites, ECF No. 44 at 7, also supports reading the ordinary course of business exception to require that the interception be instrumental to the provision of the service. A U.S. Senate Report regarding the ECPA states that "[t]he provider of electronic communications services may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain. These monitoring functions, which may be necessary to the provision of an electronic communication service, do not involve humans listening in on voice conversations. Accordingly, they are not prohibited." ECF No. 45-2 at 20. This suggests that Congress intended

---

between communications stored in the recipient's possession and those in transit is significant for the purposes of the statutory scheme as discussed *infra*.

to protect electronic communication service providers from liability when the providers were monitoring communications for the purposes of ensuring that the providers could appropriately route, terminate, and manage messages. Accordingly, the Court concludes that the legislative history supports a narrow reading of the section 2510(5)(a)(ii) exception, under which an electronic communication service provider must show some link between the alleged interceptions at issue and its ability to operate the communication system. Google's broader reading of the exception would conflict with Congressional intent.

The case law applying the "ordinary course of business" exception in the 2510(5)(a)(i) context also suggests that courts have narrowly construed that phrase. For example, in *Arias v. Mutual Central Alarm Service, Inc.*, the Second Circuit found that it was within an alarm company's ordinary course of business to record all incoming and outgoing calls because maintaining records of the calls was instrumental "to ensure that [the alarm company's] personnel are not divulging sensitive customer information, that events are reported quickly to emergency services, that customer claims regarding events are verifiable, and that the police and other authorities may rely on these records in conducting any investigations." 202 F.3d at 559 (internal quotation marks and alterations omitted). Similarly, the Tenth Circuit found that an employer's installation of a telephone monitoring device on the phone lines in departments where employees interacted with the public was within the employer's ordinary course of business because of "concern by management over abusive language used by irate customers when called upon to pay their bills, coupled with the possible need to give further training and supervision to employees dealing with the public." *James v. Newspaper Agency Corp.*, 591 F.2d 579, 581 (10th Cir. 1979).

The narrow construction of "ordinary course of business" is most evident in section 2510(5)(a)(i) cases where an employer has listened in on employees' phone calls in the workplace. *See United States v. Murdock*, 63 F.3d 1391, 1396 (6th Cir. 1995) (noting that "[a] substantial body of law has developed on the subject of ordinary course of business in the employment field where employees have sued their employers" and that "[t]hese cases have narrowly construed the phrase

'ordinary course of business'"); *Watkins*, 704 F.2d at 582. These cases suggest that an employer's eavesdropping on an employee's phone call is only permissible where the employer has given notice to the employee. *See Adams*, 250 F.3d at 984 (finding that the exception generally requires that the use be "(1) for a legitimate business purpose, (2) routine, and (3) with notice"). Further, these cases have suggested that an employer may only listen to an employee's phone call for the narrow purpose of determining whether a call is for personal or business purposes. In *Watkins*, for example, the court held that an employer "was obliged to cease listening as soon as she had determined that the call was personal, regardless of the contents of the legitimately heard conversation." 704 F.2d at 584. *Watkins* concerned a situation in which an employer listened in on an employee's personal phone call wherein the employee discussed a job interview. The Eleventh Circuit reversed a grant of summary judgment in favor of the employer notwithstanding the fact that the interception concerned a conversation that was "obviously of interest to the employer." *Id.* at 583–84.

These cases suggest a narrow reading of "ordinary course of business" under which there must be some nexus between the need to engage in the alleged interception and the subscriber's ultimate business, that is, the ability to provide the underlying service or good. In the instant matter, Plaintiffs explicitly allege that there is no comparable nexus between Google's interceptions and its ability to provide the electronic communication service at issue in this case, email. Specifically, in their Complaint, Plaintiffs state that Google's interceptions are "for [Google's] own benefit in other Google services unrelated to the service of email or the particular user." ECF No. 38-2 ¶ 97.

In light of the statutory text, case law, statutory scheme, and legislative history concerning the ordinary course of business exception, the Court finds that the section 2510(5)(a)(ii) exception is narrow and designed only to protect electronic communication service providers against a finding of liability under the Wiretap Act where the interception facilitated or was incidental to

provision of the electronic communication service at issue.[4] Plaintiffs have plausibly alleged that Google's reading of their emails was not within this narrow ordinary course of its business. Specifically, Plaintiffs allege that Google intercepts emails for the purposes of creating user profiles and delivering targeted advertising, which are not instrumental to Google's ability to transmit emails. The Consolidated Complaint alleges that "Google uses the content of the email messages [Google intercepts] and the derivative data it creates for its own benefit in other Google services unrelated to the service of email or the particular user." ECF No. 38-2 ¶¶ 97, 259(g). Plaintiffs support their assertion by suggesting that Google's interceptions of emails for targeting advertising and creating user profiles occurred independently from the rest of the email-delivery system. In fact, according to the Consolidated Complaint, the Gmail system has always had separate processes for spam filtering, antivirus protections, spell checking, language detection, and sorting than the devices that perform alleged interceptions that are challenged in this case. *Id.* ¶¶ 5, 200, 259(e). As such, the alleged interception of emails at issue here is both physically and purposively unrelated to Google's provision of email services. *Id.* ¶¶ 74, 259(g). Google's alleged interceptions are neither instrumental to the provision of email services, nor are they an incidental effect of providing these services. The Court therefore finds that Plaintiffs have plausibly alleged that the interceptions fall outside Google's ordinary course of business.

Furthermore, the D.C. Circuit has held in a section 2510(5)(a)(i) case that a defendant's actions may fall outside the "ordinary course of business" exception when the defendant violates its own internal policies. *See Berry*, 146 F.3d at 1010. In *Berry*, the court reversed a district court's grant of summary judgment in favor of the government on "ordinary course of business" grounds in part because the interception violated internal policies. That case concerned a Wiretap Act claim

[4] The Court does not find persuasive Google's slippery slope contention that a narrow interpretation of the ordinary course of business exception will make it impossible for electronic communication service providers to provide basic features, such as email searches or spam control. ECF No. 44 at 12–13. Some of these may fall within a narrow definition of "ordinary course of business" because they are instrumental to the provision of email service. Further, a service provider can seek consent to provide features beyond those linked to the provision of the service.

brought by a senior State Department officer against State Department Operations Center Watch Officers for monitoring the officer's phone call with another high-ranking officer. *Id.* at 1005. The D.C. Circuit noted that the "Operations Center Manual in effect at the time of these conversations cautioned that calls between Senior Department Officials . . . 'should not be monitored unless they so request.'" *Id.* at 1006. The court held that the "government's position [that this monitoring was within its ordinary course of business] is fatally undermined by the Operations Center guidelines which clearly indicate the norm of behavior the Watch Officers were to follow and which must be regarded as the ordinary course of business for the Center." *Id.* at 1009–10.

The Court finds that the reasoning of the D.C. Circuit applies equally in the section 2510(5)(a)(ii) context. Here, Plaintiffs allege that Google has violated its own policies and therefore is acting outside the ordinary course of business. Specifically, Plaintiffs allege that Google's Privacy Policies explicitly limit the information that Google may collect to an enumerated list of items, and that this list does not include content of emails. ECF No. 38-2 ¶¶ 187–91. Plaintiffs point to the language of the Privacy Policy that states that Google "may collect the following types of information" and then lists (1) information provided by the user (such as personal information submitted on the sign-up page), (2) information derived from cookies, (3) log information, (4) user communications to Google, (5) personal information provided by affiliated Google services and sites, (6) information from third party applications, (7) location data, and (8) unique application numbers from Google's toolbar. *Id.* ¶ 187; ECF No. 46-7. Plaintiffs further note that the updated Privacy Policy also stated that Google "collected information in two ways": "(1) information the user gives to Google—the user's personal information; and, (2) information Google obtains from the user's use of Google services, wherein Google lists: (a) the user's device information; (b) the user's log information; (c) the user's location information; (d) the user's unique application number; (e) information stored locally on the user's device; and, (e) [sic] information derived from cookies placed on a user's device." ECF No. 38-2 ¶ 189; ECF No. 46-10. Because content of emails between users or between users and non-users was not part of either

list, Plaintiffs allege that Google "violates the express limitations of its Privacy Policies." *Id.* ¶¶ 191, 195. The Court need not determine at this stage whether Plaintiffs will ultimately be able to prove that the Privacy Policies were intended to comprehensively list the information Google may collect. Rather, Plaintiffs' plausible allegations that the Privacy Policies were exhaustive are sufficient. Because Plaintiffs have alleged that Google exceeded the scope of its own Privacy Policy, the section 2510(5)(a)(ii) exception cannot apply.

Accordingly, the Court DENIES Google's Motion to Dismiss based on the section 2510(5)(a)(ii) exception.[5]

2. Consent

Google's second contention with respect to Plaintiffs' Wiretap Act claim is that all Plaintiffs consented to any interception of emails in question in the instant case. Specifically, Google contends that by agreeing to its Terms of Service and Privacy Policies, all Gmail users have consented to Google reading their emails. ECF No. 44 at 14–16. Google further suggests that even though non-Gmail users have not agreed to Google's Terms of Service or Privacy Policies, all non-Gmail users impliedly consent to Google's interception when non-Gmail users send an email to or receive an email from a Gmail user. *Id.* at 19–21.

If either party to a communication consents to its interception, then there is no violation of the Wiretap Act. 18 U.S.C. § 2511(2)(d).[6] Consent to an interception can be explicit or implied, but any consent must be actual. *See United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996);

[5] The Court notes that it is not the first court to reject Google's ordinary course of business exception theory on a motion to dismiss a challenge to the operation of Gmail. A federal district court in Texas ruled that it could not decide the question of ordinary course of business at the motion to dismiss phase. *See Dunbar v. Google, Inc.*, No. 10-CV-00194-MHS, ECF No. 61 (E.D. Tex. May 23, 2011). A state court in Massachusetts also rejected a similar claim under state law. *Marquis v. Google, Inc.*, No. 11-2808-BLSI (Mass Super. Ct. Jan. 17, 2012).

[6] However, to establish a consent defense under the state laws at issue in this case, both parties — the sender and the recipient of the communication — must consent to the alleged interception. *See* Fla. Stat. § 934.03(2)(d); Md. Code, Cts. & Jud. Proc. § 10-402(c)(3); 18 Pa. Cons. Stat. § 5704(4). Because the Court finds that no party has consented to any of the interceptions at issue in this case, the difference between the federal law's one-party consent regime and the state laws' two-party consent regimes is not relevant at this stage.

U.S. v. Amen, 831 F.2d 373, 378 (2d Cir. 1987); *U.S. v. Corona-Chavez*. 328 F.3d 974, 978 (8th Cir. 2003). Courts have cautioned that implied consent applies only in a narrow set of cases. *See Watkins*, 704 F.2d at 581 (holding that consent should not be "cavalierly implied"); *In re Pharmatak*, 329 F.3d at 20. The critical question with respect to implied consent is whether the parties whose communications were intercepted had adequate notice of the interception. *Berry*, 146 F.3d at 1011. That the person communicating knows that the interceptor has the *capacity* to monitor the communication is insufficient to establish implied consent. *Id*. Moreover, consent is not an all-or-nothing proposition. Rather, "[a] party may consent to the interception of only part of a communication or to the interception of only a subset of its communications." *In re Pharmatrack, Inc.*, 329 F.3d at 19.

In its Motion to Dismiss, Google marshals both explicit and implied theories of consent. Google contends that by agreeing to Google's Terms of Service and Privacy Policies, Plaintiffs who are Gmail users expressly consented to the interception of their emails. ECF No. 44 at 14–16. Google further contends that because of the way that email operates, even non-Gmail users knew that their emails would be intercepted, and accordingly that non-Gmail users impliedly consented to the interception. *Id.* at 19–20. Therefore, Google argues that in all communications, both parties — regardless of whether they are Gmail users — have consented to the reading of emails. *Id.* at 13–14. The Court rejects Google's contentions with respect to both explicit and implied consent. Rather, the Court finds that it cannot conclude that any party — Gmail users or non-Gmail users — has consented to Google's reading of email for the purposes of creating user profiles or providing targeted advertising.

Google points to its Terms of Service and Privacy Policies, to which all Gmail and Google Apps users agreed, to contend that these users explicitly consented to the interceptions at issue. The Court finds, however, that those policies did not explicitly notify Plaintiffs that Google would intercept users' emails for the purposes of creating user profiles or providing targeted advertising.

Section 8 of the Terms of Service that were in effect from April 16, 2007, to March 1, 2012, stated that "Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service."[7] ECF No. 46-5 at 4. This sentence was followed by a description of steps users could take to avoid sexual and objectionable material. *Id.* ("For some of the Services, Google may provide tools to filter out explicit sexual content."). Later, section 17 of the Terms of Service stated that "advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information." *Id.* at 8.

The Court finds that Gmail users' acceptance of these statements does not establish explicit consent. Section 8 of the Terms of Service suggests that content may be intercepted under a different set of circumstances for a different purpose — to exclude objectionable content, such as sexual material. This does not suggest to the user that Google would intercept emails for the purposes of creating user profiles or providing targeted advertising. *Watkins*, 704 F.2d at 582 ("[C]onsent within the meaning of section 2511(2)(d) is not necessarily an all or nothing proposition; it can be limited. It is the task of the trier of fact to determine the scope of the consent and to decide whether and to what extent the interception exceeded that consent."); *In re Pharmatrack, Inc.*, 329 F.3d at 19 ("Thus, a reviewing court must inquire into the dimensions of the consent and then ascertain whether the interception exceeded those boundaries.") (internal quotation marks omitted). Therefore, to the extent that section 8 of the Terms of Service establishes consent, it does so only for the purpose of interceptions to eliminate objectionable content. The Consolidated Complaint suggests, however, that Gmail's interceptions for the purposes of targeted advertising and creation of user profiles was separate from screening for any objectionable content. *See* ECF No. 38-2 ¶¶ 5, 200. Because the two processes were allegedly separate, consent to one does not equate to consent to the other.

[7] It is undisputed that the term "Service" throughout Google's Terms of Service includes Gmail.

Section 17 of the Terms of Service — which states that Google's "advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information" — is defective in demonstrating consent for a different reason: it demonstrates only that Google has the *capacity* to intercept communications, not that it will. *Berry*, 146 F.3d at 1011 (holding that knowledge of defendant's capacity to monitor is insufficient to establish consent). Moreover, the language suggests only that Google's advertisements were based on information "stored on the Services" or "queries made through the Services" — not information in transit via email. Plaintiffs here allege that Google violates the Wiretap Act, which explicitly protects communications in transit, as distinguished from communications that are stored. Furthermore, providing targeted advertising is only one of the alleged reasons for the interceptions at issue in this case. Plaintiffs also allege that Google intercepted emails for the purposes of creating user profiles. *See* ECF No. 38-2 ¶ 95. Section 17, to the extent that it suggests interceptions, only does so for the purposes of providing advertising, not creating user profiles. Accordingly, the Court finds that neither section of the Terms of Service establishes consent.

The Privacy Policies in effect from August 8, 2008, to October 3, 2010, to which all Gmail users agreed and upon which Google now relies, do not clarify Google's role in intercepting communications between its users. The Policies stated that Google may collect "[i]nformation you provide, [c]ookies[,] [l]og information[,] [u]ser communications to Google[,] [a]ffiliated sites, [l]inks[,] [and] [o]ther sites." *See* ECF No. 46-7 at 2–3. Google described that it used such information for the purposes of "[p]roviding our services to users, including the display of customized content and advertising." *Id.* at 3. In 2010, Google later updated the Policy to state that the collected information would be used to "[p]rovide, maintain, protect, and improve our services (including advertising services) and develop new services." *See* ECF No. 46-9 at 3. Nothing in the Policies suggests that Google intercepts email communication in transit between users, and in fact, the policies obscure Google's intent to engage in such interceptions. The Privacy Policies explicitly state that Google collects "user communications . . . *to Google*." *See*

ECF No. 46-7 at 3 (emphasis added). This could mislead users into believing that user communications to each other or to nonusers were not intercepted and used to target advertising or create user profiles. As such, these Privacy Policies do not demonstrate explicit consent, and in fact suggest the opposite.

After March 1, 2012, Google modified its Terms of Service and Privacy Policy. The new policies are no clearer than their predecessors in establishing consent. The relevant part of the new Terms of Service state that when users upload content to Google, they "give Google (and those [Google] work[s] with) a worldwide license to use . . ., create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), . . . and distribute such content." *See* ECF No. 46-6 at 3. The Terms of Service cite the new Privacy Policy, in which Google states to users that Google "may collect information about the services that you use and how you use them, like when you visit a website that uses our advertising services or you view and interact with our ads and content. This information includes: [d]evice information[,] [l]og information[,] [l]ocation information[,] [u]nique application numbers[,] [l]ocal storage[,] [c]ookies[,] and anonymous identifiers." ECF No. 46-10 at 3. The Privacy Policy further states that Google "use[s] the information [it] collect[s] from all [its] services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and [its] users. [Google] also use[s] this information to offer you tailored content — like giving you more relevant search results and ads." *See* ECF No. 46-10 at 3. These new policies do not specifically mention the content of users' emails to each other or to or from non-users; these new policies are not broad enough to encompass such interceptions. Furthermore, the policies do not put users on notice that their emails are intercepted to create user profiles. The Court therefore finds that a reasonable Gmail user who read the Privacy Policies would not have necessarily understood that her emails were being intercepted to create user profiles or to provide targeted advertisements. Accordingly, the Court finds that it cannot conclude at this phase that the new policies demonstrate that Gmail user Plaintiffs consented to the interceptions.

Finally, Google contends that non-Gmail users — email users who do not have a Gmail account and who did not accept Gmail's Terms of Service or Privacy Policies — nevertheless impliedly consented to Google's interception of their emails to and from Gmail users, and to Google's use of such emails to create user profiles and to provide targeted advertising. ECF No. 44 at 19–20. Google's theory is that all email users understand and accept the fact that email is automatically processed. *Id.* However, the cases Google cites for this far-reaching proposition hold only that the sender of an email consents to the intended recipients' recording of the email — not, as has been alleged here, interception by a third-party service provider. *See State v. Townsend*, 57 P.3d 255, 260 (Wash. 2002) (finding consent and therefore no violation of Washington's privacy act when email and instant message communications sent to an undercover police officer were used against criminal defendant); *State v. Lott*, 879 A.2d 1167, 1172 (N.H. 2005) (same under New Hampshire law); *Commonwealth v. Proetto*, 771 A.2d 823, 829 (Pa. Super. Ct. 2001) (holding that the Pennsylvania anti-wiretapping law was not violated when the recipient forwarded emails and chat messages to the police). Google has cited no case that stands for the proposition that users who send emails impliedly consent to interceptions and use of their communications by third parties other than the intended recipient of the email. Nor has Google cited anything that suggests that by doing nothing more than receiving emails from a Gmail user, non-Gmail users have consented to the interception of those communications. Accepting Google's theory of implied consent — that by merely sending emails to or receiving emails from a Gmail user, a non-Gmail user has consented to Google's interception of such emails for any purposes — would eviscerate the rule against interception. *See Watkins*, 704 F.2d at 581 ("It would thwart th[e] policy [of protecting privacy] if consent could routinely be implied from circumstances.").[8] The Court does

[8] In their briefs, the parties dispute whether members of the putative class of Gmail users who are minors consented to the interceptions. Google contends that minors are bound by the Terms of Service and Privacy Policies. ECF No. 44 at 16–17. Google argues that the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–08, preempts any state law that would have rendered the minors' consent ineffective. The Court need not reach the issue of whether minors are bound by the Terms of Service or the Privacy Policies because the Court concludes that even if the minors

not find that non-Gmail users who are not subject to Google's Privacy Policies or Terms of Service have impliedly consented to Google's interception of their emails to Gmail users.

Because Plaintiffs have adequately alleged that they have not explicitly or implicitly consented to Google's interceptions, the Court DENIES Google's Motion to Dismiss on the basis of consent.[9]

B. CIPA

CIPA, Cal. Penal Code § 630, *et seq.*, California's anti-wiretapping and anti-eavesdropping statute, prohibits unauthorized interceptions of communications in order "to protect the right of privacy." Cal. Penal Code § 630. The California Legislature enacted CIPA in 1967 in response to "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications." *Id.*

Section 631 prohibits wiretapping or "any other unauthorized connection" with a "wire, line, cable, or instrument." *See* Cal. Penal Code § 631(a). The California Supreme Court has held that section 631 protects against three distinct types of harms: "intentional wiretapping, willfully attempting to learn the contents or meaning of a communication in transit over a wire, and attempting to use or communicate information obtained as a result of engaging in either of the previous two activities." *Tavernetti v. Superior Court*, 583 P.2d 737, 741 (Cal. 1978). Section 632 prohibits unauthorized electronic eavesdropping on confidential conversations. *See* Cal. Penal Code § 632(a). To state a claim under section 632, a plaintiff must allege an electronic recording

---

are subject to these agreements, the agreements did not establish consent. Similarly, Google contends that Google Apps users are also bound by the Terms of Service and Privacy Policies even though they were required by their educational institutions or ISPs to use Gmail. ECF No. 44 at 17–18. Again, because the Court concludes that the agreements did not establish consent, the Court need not reach the issue of whether Google Apps users are bound by the agreements.

[9] Other courts have also rejected Google's consent defense against state and federal anti-wiretapping challenges to the operation of Gmail. *See Dunbar v. Google, Inc.*, No. 10-cv-00194-MHS, ECF No. 61 (E.D. Tex. May 23, 2011); *Marquis v. Google, Inc.*, No. 11-2808-BLSI (Mass Super. Ct. Jan. 17, 2012).

of or eavesdropping on a confidential communication, and that not all parties consented to the eavesdropping. *Flanagan v. Flanagan*, 41 P.3d 575, 577 (Cal. 2002).

CIPA also contains a public utility exemption, which applies to claims under both sections 631 and 632. Cal. Penal Code §§ 631(b), 632(e). Neither section applies "to any public utility engaged in the business of providing communications services and facilities, or to the officers, employees, or agents thereof, where the acts otherwise prohibited by this section are for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility." Cal. Penal Code §§ 631(b), 632(e).

Plaintiffs allege violations of both section 631 and section 632. *See* ECF No. 38-2 ¶ 321. Google moves to dismiss on five bases. *See* ECF No. 44 at 23–24, 27–28. Google contends that Plaintiffs lack standing to allege such violations and that the California law should not apply due to choice of law principles. *See id*. Google also moves to dismiss Plaintiffs' claims on substantive bases, contending that neither section 631 nor section 632 applies to email and that the public utility exemption applies. *See* ECF No. 44 at 21–23, ECF No. 56 at 14–15. Finally, Google moves to dismiss Plaintiffs' section 632 claim because the communications at issue in this case were not confidential as defined by that section and because that section is preempted by the ECPA. *See* ECF No. 44 at 25–27.

1. Standing

Google first contends that Plaintiffs lack standing under Article III to assert a CIPA claim. A federal court must ask whether a plaintiff has suffered sufficient injury to satisfy the "case or controversy" requirement of Article III of the U.S. Constitution. ECF No. 44 at 23–24. To satisfy Article III standing, a plaintiff must allege: (1) injury-in-fact that is concrete and particularized, as well as actual or imminent; (2) wherein injury is fairly traceable to the challenged action of the defendant; and (3) it is likely (not merely speculative) that injury will be redressed by a favorable decision. *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180–81 (2000); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). A suit brought by a plaintiff

without Article III standing is not a "case or controversy," and an Article III federal court therefore lacks subject matter jurisdiction over the suit.

Google's contention is that Plaintiffs have not suffered the "injury" required by Article III to confer standing. ECF No. 44 at 24. Under Ninth Circuit precedent, the injury required by Article III may exist by virtue of "statutes creating legal rights, the invasion of which creates standing." *See Edwards v. First Am. Fin. Corp.*, 610 F.3d 514, 517 (9th Cir. 2010) (quoting *Warth v. Seldin*, 422 U.S. 490, 500 (1975)). In such cases, the "standing question . . . is whether the constitutional or statutory provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief." *Id.* (quoting *Warth*, 422 U.S. at 500). In *Edwards*, the Ninth Circuit has held that the Real Estate Settlement Procedures Act ("RESPA") conferred standing to a homeowner who sought to challenge the kickback relationship between the title insurer and title agency despite the fact that the homeowner suffered no independent injury, through, for example, overpayment. *Id.* The court there held that the structure of RESPA was such that independent injury was not needed; a plaintiff's showing that the defendant's conduct violated the statute was sufficient to confer standing. *Id.* [10]

Applying the Ninth Circuit's decision in *Edwards*, courts in this district have found that allegations of a Wiretap Act violation are sufficient to establish standing. In *In re Facebook Privacy Litigation*, 791 F. Supp. 2d 705, 712 (N.D. Cal. 2011), for example, the court held that the "Wiretap Act provides that any person whose electronic communication is 'intercepted, disclosed, or intentionally used' in violation of the Act may in a civil action recover from the entity which engaged in that violation." Accordingly, the court found that where the plaintiffs had alleged that

[10] The United States Supreme Court granted a petition for a writ of certiorari in *Edwards* on the question of whether statutory injury alone could confer standing under Article III even though the Courts of Appeal that had considered the question had unanimously concluded that allegations of RESPA violations alone sufficed for standing. *See First Am. Fin. Corp. v. Edwards*, 131 S. Ct. 3022 (2011). After oral argument, however, the Supreme Court dismissed the writ as improvidently granted. *See First Am. Fin. Corp. v. Edwards*, 132 S. Ct. 2536 (2012). This left in place the Ninth Circuit's decision in *Edwards*, which remains binding authority that this Court must apply, as it does here.

their communications had been intercepted, they "alleged facts sufficient to establish that they have suffered the injury required for standing under Article III." *Id.* at 712; *see also In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1055 (N.D. Cal. 2012) ("[A] violation of the Wiretap Act . . . may serve as a concrete injury for the purposes of Article III injury analysis."); *In re Google, Inc. Privacy Policy Litig.*, 2012 WL 6738343 (N.D. Cal. Dec. 28, 2012) ("[If viable], Plaintiffs' Wiretap Act claim might help [show standing], [because] a violation of the rights provided under the statute may be sufficient by itself to confer standing.")

The reasoning of these cases that find standing when there is an allegation of a Wiretap Act violation applies equally to CIPA. Like the Wiretap Act, CIPA creates a private right of action when a defendant engages in wiretapping or eavesdropping. *Compare* 18 U.S.C. § 2520(a) ("[A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation), *with* Cal. Penal Code § 637.2(a) ("Any person who has been injured by a violation of this chapter may bring an action against the person who committed the violation."). Further, like the Wiretap Act, CIPA authorizes an award of statutory damages any time a defendant violates the provisions of the statute without any need to show actual damages. *Compare* 18 U.S.C. § 2520(c) (authorizing statutory damages), *with* Cal. Penal Code § 637.2(a)(1) (same) *and* Cal. Penal Code § 637.2(c) ("It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."). Therefore, the Court finds that the allegation of a violation of CIPA, like an allegation of the violation of the Wiretap Act, is sufficient to confer standing without any independent allegation of injury. Like both RESPA and the Wiretap Act, therefore, CIPA creates a statutory right the violation of which confers standing on a plaintiff.

Google relies exclusively on the differences in statutory text between CIPA and the Wiretap Act to contend that CIPA requires an independent allegation of injury even where the Wiretap Act does not. Specifically, Google notes that the provision of CIPA that creates a cause of action states

that, "[a]ny person who *has been injured* by a violation of this chapter may bring an action against the person who committed the violation." Cal. Penal Code § 637.2(a) (emphasis added). Google's contention is that the word "injured" means that Plaintiffs must show some injury independent of the invasion of their statutory rights under CIPA. Google cites no authority for the proposition that section 637.2 requires independent injury or the proposition that the word "injured" triggers an obligation to demonstrate independent injury for the purposes of Article III standing. The California case law on CIPA cuts against Google's contention that "injured" requires independent injury. As the California Court of Appeals has stated, "Section 637.2 is fairly read as establishing that no violation of the Privacy Act [CIPA] is to go unpunished. Any invasion of privacy involves an affront to human dignity which the Legislature could conclude is worth at least $3,000. The right to recover this statutory minimum accrued at the moment the Privacy Act [CIPA] was violated." *Friddle v. Epstein*, 21 Cal. Rptr. 85, 92 (Cal Ct. App. 1993); *see also id.* ("Plaintiff invaded defendants' privacy and violated the Privacy Act [CIPA] at the moment he began making his secret recording. No subsequent action or inaction is of consequence to this conclusion."); *accord Ribas v. Clark*, 38 Cal. 3d 355, 365 (Cal. 1985) ("In view of the manifest legislative purpose to accord every citizen's privacy the utmost sanctity, section 637.2 was intended to provide those who suffer an infringement of this aspect of their personal liberty a means of vindicating their right.").

Accordingly, the Court finds that CIPA and the Wiretap Act are not distinguishable for the purposes of standing. Because courts have, under existing Ninth Circuit authority, consistently held that the invasion of rights under the Wiretap Act is sufficient for Article III standing, this Court concludes that the same is true of CIPA. All Plaintiffs need allege is an invasion of statutory CIPA rights to survive a motion to dismiss on standing grounds. There is no dispute that they have done so here. The Court therefore DENIES Google's Motion to Dismiss the CIPA claims on standing grounds.

2. Choice of Law

Google contends that under choice of law principles, California law should not apply and that the Court should accordingly dismiss Plaintiffs' California claims. ECF No. 44 at 27–30. Plaintiffs contend that the choice of law analysis should wait for later stages of the proceedings. ECF No. 53 at 28. As set forth below, the choice of law inquiry raises complicated, fact-intensive questions better answered at later stages of the litigation. Therefore, the Court DENIES the Motion to Dismiss on choice of law grounds.

To determine which state's law should apply, "[a] federal court . . . must look to the forum state's choice of law rules to determine the controlling substantive law." *Mazza v. American Honda Motor Co., Inc.*, 666 F.3d 581, 589 (9th Cir. 2012) (internal quotation marks omitted). Under California law, class action plaintiffs have the burden to "show that California has sufficient contact or sufficient aggregation of contacts to the claims of each class member." *Id*. at 589–90 (internal quotation marks omitted). If this showing is made, "the burden shifts to the other side to demonstrate that foreign law, rather than California law, should apply to class claims." *Id*. at 590.

"California courts apply the so-called governmental interest analysis" to determine whether California law should be applied on a class-wide basis." *Kearney v. Salomon Smith Barney, Inc.*, 137 P.3d 914, 917 (Cal. 2006). Under this three-part test: "[1] the court determines whether the relevant law of each of the potentially affected jurisdictions with regard to the particular issue in question is the same or different . . .[; 2] if there is a difference, the court examines each jurisdiction's interest in the application of its own law under the circumstances of the particular case to determine whether a true conflict exists . . . [; and 3] if the court finds there is a true conflict, it carefully evaluates and compares the nature and strength of the interest of each jurisdiction in the application of its own law . . . and then ultimately applies the law of the state whose interest would be more impaired if its law were not applied." *Mazza*, 666 F.3d at 590 (quoting *McCann v. Foster Wheeler, LLC*, 225 P.3d 517, 527 (Cal. 2010)).

The Court finds that Plaintiffs have established that their claims are sufficiently related to California to trigger application of the three-part test. The Ninth Circuit has held that sufficient aggregate contacts with California are established in a class action when a defendant's corporate headquarters is located in the state, advertising materials pertaining to representations the company made to class members are created in the state, and one fifth of the class is located in California. *Mazza*, 666 F.3d at 590. In this case, as Plaintiffs allege, Google is located in California, it developed and implemented the practices at issue in this action in California, and one or more of the physical interceptions at the heart of Plaintiffs' claims occurred in California. ECF No. 38-2 ¶ 290 ("Google's acts in violation of CIPA occurred in the State of California . . . . Google's implementation of its business decisions, practices, and standard ongoing policies which violate CIPA took place in the State of California. Google profited in the State of California"); ECF No. 53 at 29. In short, California is the epicenter of the practices at issue in this case for all Plaintiffs. Therefore, the Court finds that Plaintiffs have shown that "California has a constitutionally sufficient aggregation of contacts to the claims of each putative class member." *Mazza*, 666 F.3d at 590.

Because the Court finds sufficient aggregate contacts, it turns to the first of the three-part inquiry to determine whether California law or the law of another state should apply to the class claims. The Court must determine whether there is a material conflict between the laws of California and those of the Plaintiffs' home states. Google contends that there is a conflict because Alabama and Maryland law are narrower with respect to scope of liability, enforcement mechanisms, and available remedies. ECF No. 44 at 28.

The Court cannot, at this stage, determine whether there are differences with respect to the scope of liability. Google correctly contends that under Alabama and Maryland's law, one party's consent is sufficient to negate an interception, while under California law, both parties must consent. *Id.* Yet, it is not clear whether this difference in the scope of liability is material, that is whether, it "make[s] a difference in this litigation." *Mazza*, 666 F.3d at 590. This is because

Plaintiffs contend that neither party has consented, while Google contends that all parties have consented. ECF No. 38-2 ¶ 102–97, ECF No. 44 at 13–14. Accordingly, on either party's theory of liability, the difference in state law with respect to the consent standard would not be a material difference.

Therefore, the Court finds that it cannot conduct a meaningful choice of law analysis, such as that contemplated by *Mazza*, at this early stage of the litigation where the issues of contention are still in flux.[11] As other courts have noted, the rigorous choice of law analysis required by *Mazza* cannot be conducted at the motion to dismiss stage. *See Clancy v. The Bromley Tea Co.*, 2013 WL 4081632 (N.D. Cal. Aug. 9, 2013) ("Such a detailed choice-of-law analysis is not appropriate at [the motion for judgment on the pleadings] stage of the litigation. Rather, such a fact-heavy inquiry should occur during the class certification stage, after discovery."); *In re Clorox Consumer Litig.*, 894 F. Supp. 2d 1224, 1237 (N.D. Cal. 2012) ("Significantly, *Mazza* was decided on a motion for class certification, not a motion to strike. At [the motion to dismiss] stage of the instant litigation, a detailed choice-of-law analysis would be inappropriate. Since the parties have yet to develop a factual record, it is unclear whether applying different state consumer protection statutes could have a material impact on the viability of Plaintiffs' claims.") (citation omitted); *Donohue v. Apple, Inc.*, 871 F. Supp. 2d 913, 923 (N.D. Cal. 2012) ("Although *Mazza* may influence the decision whether to certify the proposed class and subclass, such a determination is premature. At [the motion to dismiss] stage in the litigation—before the parties have submitted briefing regarding either choice-of-law or class certification—plaintiff is permitted to assert claims under the laws of different states in the alternative."); *In re Sony Grand Wega KDF-E A10/A20 Series Rear Projection HDTV Television Litig.*, 758 F. Supp. 2d 1077, 1096 (S.D. Cal. 2010) ("In a

[11] The Court recognizes that additional conflicts may arise out of California's acknowledgement of a private right of action and/or the remedies California allows under CIPA. However, under California choice of law analysis, differences in remedies alone are not dispositive. The Court may resolve the conflict between California and foreign law by "apply[ing] California law in a restrained manner" with regard to monetary damages. *Kearney*, 39 Cal. 4th at 100–01. In any case, the Court will resolve all conflict of law questions at the class certification stage.

putative class action, the Court will not conduct a detailed choice-of-law analysis during the pleading stage.").

Accordingly, the Court defers resolution of the choice of law issues until the class certification phase and DENIES Google's Motion to Dismiss on the basis of choice of law without prejudice to Google raising this argument at a later stage.

3. Section 631

Google contends that even if Plaintiffs' section 631 challenge is not procedurally barred, it is substantively deficient because that section does not apply to emails. ECF No. 44 at 21–23. Further, in its reply brief, Google contends that the public utility exemption applies. ECF No. 56 at 14–15.

a. Application to Email

The Court finds that there is no binding authority with respect to whether section 631 applies to email.[12] The only authority from the California courts is a Superior Court ruling. *See Diamond v. Google, Inc.*, CIV-1202715 (Cal. Super. Ct., Marin Cnty. Aug. 14, 2013) (finding, without providing analysis, that allegations of interception of email communication are sufficient to state a claim under Cal. Penal Code § 631). While two federal courts have been confronted with the application of CIPA to Internet browsing history and emails, those matters were resolved on other grounds before reaching the question of CIPA's application to digital technologies generally or email specifically. *Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022 (N.D. Cal. 2011); *Bradley v. Google*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006).

In the absence of binding authority, this Court must predict what the California Supreme Court would do if confronted with this issue. *See Valentine*, 804 F. Supp. 2d at 1027. The Court begins by looking to the text. Section 631 establishes liability for:

[12] California courts have, however, applied section 632 to internet communication technologies. *See People v. Nakai*, 183 Cal. App. 4th 499 (2010); *People v. Cho*, 2010 WL 4380113 (Cal. Ct. App. Nov. 5, 2010); *People v. Griffitt*, 2010 WL 5006815 (Cal. Ct. App. Dec. 9, 2010).

> [a]ny person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraphic or telephone wire, line cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully or without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable, or is being sent from, or received at any place within this state.

Cal. Penal Code § 631. Google contends that the language "reads or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable" applies only to interception of content on *telephone and telegraphic* wires, lines, or cables, as the first clause of the statute describes. ECF No. 44 at 21. As a result, Google contends that the second clause, upon which Plaintiffs rely, cannot apply to email since emails are not messages, reports or communications that pass over telephone or telegraphic wires. *Id.*

The Court rejects Google's reading of the statute. As a threshold matter, the second clause of the statute, which creates liability for individuals who "read[] or attempt[] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over *any* wire, line or cable, or is being sent from, or received at any place within this state[,]" is not limited to communications passing over "telegraphic or telephone" wires, lines, or cables. *See* Cal. Penal Code § 631 (emphasis added). Furthermore, the Court finds no reason to conclude that the limitation of "telegraphic or telephone" on "wire, line, cable, or instrument" in the first clause of the statute should be imported to the second clause of the statute. The second clause applies only to "wire[s], line[s], or cable[s]" — not "instrument[s,]" which are included in the first clause. The Court finds that this difference in coverage between the first and second clauses suggests that the Legislature intended the two clauses to apply to different types of communications. Accordingly, the Court rejects Google's contention that the limitations in the first clause must also apply to the second clause. The Court therefore finds that the plain language of the statute is broad enough to encompass email.

Further, the California Supreme Court's repeated finding that the California legislature intended for CIPA to establish broad privacy protections supports an expansive reading of the statute. *See Flanagan*, 41 P.3d at 581 ("In enacting [CIPA], the Legislature declared in broad terms its intent to protect the right of privacy of the people of this state from what it perceived as a serious threat to the free exercise of personal liberties. This philosophy appears to lie at the heart of virtually all the decisions construing [CIPA]."") (internal quotation marks and citations omitted); *Ribas v. Clark*, 696 P.2d 637, 641 (Cal. 1985) (finding it is "probable" that the legislature designed Section 631 as a catch all to "proscrib[e] attempts to circumvent other aspects of the Privacy Act, e.g., by requesting a secretary to secretly transcribe a conversation over an extension, rather than tape recording it in violation of section 632"); *Tavernetti v. Superior Court*, 583 P.2d 737, 742 (Cal. 1978) ("Th[e] forceful expression of the constitutional stature of privacy rights [in California] reflects a concern previously evinced by the Legislature in enacting the invasion of privacy provisions of the Penal Code.").

Moreover, the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme. For example, in a previous evolution in communications technology, the California Supreme Court interpreted "telegraph" functionally, based on the type of communication it enabled. In *Davis v. Pacific Telephone & Telegraph*, the Supreme Court held that "*telegraph* lines" in a criminal law proscribing the cutting of lines included *telephone* lines because "[t]he idea conveyed by each term is the sending of intelligence to a distance . . . [thus] the term 'telegraph' means any apparatus for transmitting messages by means of electric currents and signals." *Davis v. Pacific Telephone & Telegraph Co.*, 59 P. 698, 699 (Cal. 1899); *see also Apple v. Superior Court*, 292 P.2d 883, 887 (Cal. 2013) ("Fidelity to legislative intent does not make it impossible to apply a legal text to technologies that did not exist when the text was created." (internal quotation marks omitted)).

In line with the plain language of the statute, the California Supreme Court's pronouncements regarding the broad legislative intent underlying CIPA to protect privacy, and the

California courts' approach to updating obsolete statutes in light of emerging technologies, the Court finds that section 631 of CIPA applies to emails.

b. Public Utility Exemption

Google contends that even if CIPA applies to emails, it is a "public utility" that is exempt from the statute. ECF No. 56 at 14–15. The Court declines to reach this conclusion. California's Constitution defines "public utilities" as "[p]rivate corporations and persons that own, operate, control, or manage a line, plant, or system for . . . the transmission of telephone and telegraph messages . . . directly or indirectly to or for the public." Cal. Const., art. XII, § 3. The California Public Utility Code further defines this definition of "public utility" as "every common carrier . . . , telephone corporation [or] telegraph corporation . . ., where the service is performed for, or the commodity is delivered to, the public or any portion thereof." Cal. Pub. Util. Code § 216(a). The Public Utility Code further specifies that a "telegraph corporation" is "every corporation or person *owning, controlling, operating, or managing* any telegraph line for compensation within this State." *Id.* § 236 (emphasis added). "Telegraph line" is defined as "all conduits, ducts, poles, wires, cables, instruments, and appliances, and all other real estate, fixtures, and personal property owned, controlled, operated, or managed in connection with or to facilitate communication by telegraph, whether such communication is had with or without the use of transmission wires." *Id.* § 235. The code uses analogous definitions for "telephone corporations" and "telephone lines." *Id.* §§ 233, 234.

In short, in California, a "public utility" is a precisely defined entity subject to an expansive and exacting regulatory regime. Under the plain language of the statutes, merely operating a service over a telephone or telegraph line does not render a company a public utility. Rather, the critical question is whether the company owns, controls, operates or manages a telephone or telegraph line. Cal. Pub. Util. Code § 236. Nothing in the record suggests that Google owns, controls, operates, or manages a telephone or telegraph lines in California. Accordingly, the Court finds that Google is not a "public utility" and thus does not qualify for the public utility exemption

of Cal. Penal Code §§ 631(b). The Court therefore DENIES Google's Motion to Dismiss Plaintiffs' section 631 claims.

4. Section 632

To state a claim under California Penal Code § 632, a plaintiff must prove (1) an electronic recording of or eavesdropping on (2) a "confidential communication" (3) to which all parties did not consent. *Flanagan*, 41 P.3d at 577. As set forth below, Plaintiffs have not established that the communications at issue are confidential pursuant to section 632. Accordingly, the Court GRANTS without prejudice Google's Motion to Dismiss Plaintiffs' section 632 claim. Because this second element of a section 632 claim is not met, the Court need not address whether email constitutes an electronic recording under the statute nor need it address whether there was consent under California law.[13]

A conversation is "confidential" under section 632 "if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded . . . . The standard of confidentiality is an objective one defined in terms of reasonableness." *Faulkner v. ADT Sec. Servs., Inc.*, 706 F.3d 1017, 1019 (9th Cir. 2013). "To prevail against a 12(b)(6) motion, then, [the plaintiff] would have to allege facts that would lead to the plausible inference that his was a confidential communication — that is, a communication that he had an objectively reasonable expectation was not being recorded." *Id.* at 1020.

There is no authority from the California courts addressing whether emails can be confidential communication. Some decisions from the California appellate courts, however, suggest that internet-based communication cannot be confidential. These courts rely on the theory that individuals cannot have a reasonable expectation that their online communications will not be recorded. In *People v. Nakai*, 107 Cal. Rptr. 3d 402 (Cal. Ct. App. 2010), for example, the California Court of Appeals found that section 632 did not protect instant message communications

[13] The Court also need not address whether the ECPA preempts section 632 of CIPA, as Google contends. *See* ECF No. 44 at 26–27.

of a criminal defendant charged with attempting to send harmful matter to a minor with intent to arouse and seduce. There, the defendant, an adult man, had sent sexually explicit material via instant message to a 35-year-old decoy, who was posing as a 12-year-old girl. *Id.* at 405–07. The appellate court found that while the defendant intended that the communication be kept confidential between himself and the recipient, he could not reasonably expect that the communications would not be recorded. *Id.* at 418. Specifically, the court found that the fact that the intended recipient could easily forward the information to others militated against finding that there was a reasonable expectation that the instant message would be kept confidential. *Id.* As the court stated, "it was not reasonable for defendant to expect the communications to be confidential because the circumstances reflect that the communications could have easily been shared or viewed by . . . any computer user with whom [the intended recipient] wanted to share the communication." *Id.*; *see also People v. Cho*, 2010 WL 4380113 (Cal. Ct. App. Nov. 5, 2010) (holding chat conversations are not confidential under section 632); *People v. Griffitt*, 2010 WL 5006815 (Cal. Ct. App. Dec. 9, 2010) ("Everyone who uses a computer knows that the recipient of e-mails and participants in chat rooms can print the e-mails and chat logs and share them with whoever they please, forward them or otherwise send them to others.").

The Court finds that Plaintiffs have not alleged facts that lead to the plausible inference that the communication was not being recorded because email by its very nature is more similar to internet chats. Unlike phone conversations, email services are by their very nature recorded on the computer of at least the recipient, who may then easily transmit the communication to anyone else who has access to the internet or print the communications. Thus, Plaintiffs have not plausibly alleged that they had an objectively reasonable expectation that their email communications were "confidential" under the terms of section 632.[14]

[14] The Court's holding that the emails are not "confidential" under section 632 is consistent with the conclusion that Plaintiffs have nevertheless not consented to Google's interceptions under the Wiretap Act and state analogues. *See supra* section III.A.2. Determining whether a communication is confidential under section 632 requires the Court to look to whether the intended

Therefore, the Court GRANTS Google's Motion to Dismiss Plaintiffs' section 632 claims. In a case concerning whether a communication was confidential under section 632, the Ninth Circuit affirmed a district court's grant of a defendant's motion to dismiss, but "[i]n an abundance — perhaps an overabundance — of caution" remanded "to the district court for it to consider allowing the plaintiff to amend his complaint in a manner that would satisfy federal pleading standards." *Faulkner*, 706 F.3d at 1021. Here too this Court in "an abundance of caution" grants Plaintiffs' leave to amend their Consolidated Complaint. *Id.*; Fed. R. Civ. Proc. 15(a).

C. Other State Law Claims

Plaintiffs also allege that Google violated Pennsylvania, Maryland, and Florida law. With respect to Maryland and Florida law, Google's sole contention in its Motion to Dismiss is that these claims are derivative of Plaintiffs' federal causes of action. *See* ECF No. 44 at 5. Google expressly acknowledges that the Maryland and Florida anti-wiretapping statutes mirror the ECPA. *See id.* Therefore, Google's Motion to Dismiss these claims is based on its Motion to Dismiss Plaintiffs' federal claims. Because the Court denies Google's Motion to Dismiss Plaintiffs' federal causes of action, the Court also DENIES Google's Motion to Dismiss Plaintiffs' Maryland and Florida claims.

Google offers an independent basis for dismissing part of Plaintiff's Pennsylvania law cause of action. Specifically, Google contends that Pennsylvania law protects only the sender of communication from wiretapping, not the recipient of that communication. *See* ECF No. 44 at 13. As a result, Google moves to dismiss Plaintiffs' Pennsylvania law claim brought by those who received emails from Gmail addresses. *Id.*

---

recipient of the communication is likely to share the communication. In contrast, the question of consent turns on whether Plaintiffs have authorized the third-party interceptor's interference in the communication. In the instant matter, the Court concludes that emails are not likely to be kept confidential by the intended recipients under section 632. Nevertheless, individuals do not consent to third parties' interception of their emails.

Google relies on *Klump v. Nazareth Area Sch. Dist.*, 425 F. Supp. 2d 622, 633 (E.D. Pa. 2006), where the court held that "[a] claimant must demonstrate 'that he engaged in [a] communication'. The intended recipient of an intercepted communication, therefore, has no standing to raise claim [sic] under section 5725." *See* ECF No. 44 at 13. Plaintiffs do not contest that *Klump* limits the scope of their Pennsylvania cause of action to those who sent emails to Gmail recipients and eliminates their cause of action against those who received emails from Gmail senders. Rather, Plaintiffs contend only that this Court should not follow *Klump* because that case was wrongly decided. *See* ECF No. 53 at 11. However, Plaintiffs do not point to any authority from the state or federal courts in Pennsylvania that is contrary to the court's holding in *Klump*. In the absence of contrary authority, this Court will follow the decision in *Klump*. Accordingly, the Court GRANTS Google's Motion to Dismiss with respect to the claims under Pennsylvania law raised by Plaintiffs who received emails from Gmail users. In an abundance of caution, however, the Court grants Plaintiffs leave to amend the Consolidated Complaint.

V. CONCLUSION

For the foregoing reasons, the Court hereby GRANTS Google's Motion to Dismiss with leave to amend with respect to Plaintiffs' CIPA section 632 claims and Plaintiffs' Pennsylvania law claim as it relates those who received emails from Gmail users. The Court DENIES Google's Motion to Dismiss with respect to all other claims. Plaintiffs shall file any amended complaint within 21 days of this order. Plaintiffs may not add new causes of action or parties without a stipulation or order of the Court under Rule 15 of the Federal Rules of Civil Procedure. Failure to cure deficiencies will result in dismissal with prejudice.

IT IS SO ORDERED.

Dated: September 26, 2013

Lucy H. Koh

LUCY H. KOH
United States District Judge

COOLEY LLP
MICHAEL G. RHODES (116127) (rhodesmg@cooley.com)
WHITTY SOMVICHIAN (194463) (wsomvichian@cooley.com)
KYLE C. WONG (224021) (kwong@cooley.com)
101 California Street, 5th Floor
San Francisco, CA 94111-5800
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

Attorneys for Defendant
GOOGLE INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE GOOGLE INC. GMAIL LITIGATION

THIS DOCUMENT RELATES TO:
ALL ACTIONS

Case No. 5:13-md-02430-LHK

DEFENDANT GOOGLE INC.'S MOTION TO DISMISS PLAINTIFFS' CONSOLIDATED INDIVIDUAL AND CLASS ACTION COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

F.R.C.P. 12(b)(1), 12(b)(6)

Date: September 5, 2013
Time: 1:30 p.m.
Judge: Hon. Lucy H. Koh
Courtroom: 8

Trial Date: Not yet set

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

TABLE OF AUTHORITIES
(continued)

Page

NOTICE OF MOTION AND MOTION TO DISMISS

PLEASE TAKE NOTICE that on September 5, 2013, at 1:30 p.m., defendant Google Inc. ("Google") will and hereby does move to dismiss Plaintiffs' Consolidated Individual and Class Action Complaint (the "Complaint"). Google's Motion to Dismiss is made pursuant to Rules 12(b)(1) and (6) of the Federal Rules of Civil Procedure, and is based on this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities and other pleadings in support of the Motion, and all pleadings on file in this matter, and upon such other matters as may be presented to the Court at the time of the hearing or otherwise.

STATEMENT OF ISSUES TO BE DECIDED

1. Have Plaintiffs stated a claim that the automated processing of email in Google's Gmail service violates the Federal Wiretap Act, as amended by the Electronic Communications Privacy Act ("ECPA"), and its Florida, Maryland, and Pennsylvania state law analogues (collectively the "wiretap statutes"), where:

- The wiretap statutes exempt providers of an electronic communication service (an "ECS") like Google from liability based on conduct in the ordinary course of business and the Complaint confirms that the alleged "interceptions" occur as part of Google's normal processes in providing the Gmail service;
- ECPA precludes liability where a single party to a communication consents to the alleged "interception," and all Gmail users contractually agree to the scanning of email as part of using Google's services;
- The state wiretap statutes preclude liability where both parties to a communication consent, and case law holds that all users of email necessarily give implied consent to the automated processing of their emails;
- The Pennsylvania wiretap statute applies only to the senders, not the recipients of, an electronic communication.

2. Have Plaintiffs stated a claim that Google's automated processing of email violates the California Invasion of Privacy Act ("CIPA"), where:

- The express terms and legislative history of CIPA confirm that the statute excludes email;
- The only Plaintiffs purporting to bring a CIPA claim are non-California residents who allege no connection with California;
- CIPA allows a claim only for injured persons and Plaintiffs allege no harm of any kind from the automated processing of their emails.

I. INTRODUCTION.

This case involves Plaintiffs' effort to criminalize ordinary business practices that have been part of Google's free Gmail service since it was introduced nearly a decade ago. While Plaintiffs are differently situated (some are Gmail users; others are non-Gmail users who exchange emails with Gmail users), their claims boil down to the same core allegation: that Google commits an illegal "interception" when it applies automated (non-human) scanning to emails involving Gmail users–even though the processes at issue are a standard and fully-disclosed part the Gmail service. This claim fails as matter of law for multiple reasons.

First, all of the federal and state wiretap laws at issue specifically exempt ECS providers from liability based on conduct in their ordinary course of business. These protections reflect the reality that ECS providers like Google *must* scan the emails sent to and from their systems as part of providing their services. While Plaintiffs go to great lengths to portray Google in a sinister light, the Complaint actually confirms that the automated processes at issue are Google's ordinary business practices implemented as part of providing the free Gmail service to the public. This is fatal to Plaintiffs' claims.

Second, the wiretap statutes also preclude liability where either a single party to the communication (for the federal statute) or both parties (for the state statutes) have expressly or impliedly consented to the practices at issue. Here, all Plaintiffs who are Gmail users consented to the automated scanning of their emails (including for purposes of delivering targeted advertising) in exchange for using the Gmail service, thus precluding any claim under federal law. Moreover, multiple courts have held that *all* email senders impliedly consent to the processing of their emails by virtue of the fact that email cannot be sent or delivered without some form of electronic processing. This combination of express and implied consent bars Plaintiffs' claims in their entirety, under both the federal and state wiretap statutes.

Third, the CIPA claim brought by certain Plaintiffs is even farther afield than the wiretapping claims above because CIPA does not apply to emails *at all*, as confirmed by both the express terms and legislative history of the statute. In fact, the California Legislature specifically considered *and rejected* proposals to expand the statute to cover emails. And even if CIPA could

be interpreted to cover emails, both implied consent and choice of law rules would preclude the CIPA Plaintiffs from relying on the statute. As residents of Alabama and Maryland whose emails have no alleged connection to California, these Plaintiffs cannot invoke the protections of California law and bypass the laws of the states in which they reside simply because they want to avoid the requirements and limitations of their local laws.

Last, Plaintiffs' claims should be rejected because they would lead to anomalous results with far-ranging consequences beyond the allegations in the Complaint. Plaintiffs' theory–that any scanning of email content by ECS providers is illegal–would effectively criminalize routine practices that are an everyday aspect of using email. Indeed, Plaintiffs' effort to carve out spam filtering and virus detection from their claims underscores the fact that their theory of liability would *otherwise* encompass these common services that email users depend on. Notwithstanding these limited carve-outs, Plaintiffs' theory would still sweep up a host of common features that benefit consumers. For example, Plaintiffs' theory of liability would prevent ECS providers from providing features that allow users to sort their emails using automated filters or even to search their emails for specific words—because these features necessarily involve the scanning of email content and would thus be an illegal "interception" under Plaintiffs' theory. The Court should not allow the Complaint to proceed on this sweeping basis.

II. STATEMENT OF FACTS.

A. Gmail.

Gmail is one of the most popular web-based email services in the world with over 400 million users. Like all email providers, Google applies automated systems for the delivery of email. As part of this processing, Google's automated systems scan email content to filter out spam, detect computer viruses, and provide various features, including functions that allow users to search their email messages, automatically sort incoming email, and others. These systems are also used to display advertisements targeted to email content, as Google has disclosed since the inception of Gmail nearly a decade ago. The revenues from these advertisements enable Google to provide the Gmail service for free to the public. Gmail's advertising-based business model is similar to that of other free email services offered by Yahoo, AOL, and Hotmail. Yahoo, the very

web-based email service one named Plaintiff uses, also generates revenue from scanning email content to deliver targeted advertising.[1] The processes related to Google's automated scanning are completely automated and involve no human review.

B. Google Apps.

"Google Apps" is a suite of Google products that includes Gmail. Google Apps enables its users–which can include businesses, educational organizations, and Internet service providers ("ISPs")–to provide email services to their employees, students, or customers.[2] These email services are operated by Gmail but can be customized in certain ways. Cable One, Inc. ("Cable One") is an ISP and the Universities of Hawaii ("Hawaii") and of the Pacific ("UoP") are two educational institutions that provide email services to their users (including Plaintiffs Dunbar, Castillo, and Fread) through Google Apps. (Compl. ¶¶ 8, 14, 100, 101.)

C. Google's Terms and Disclosures.

The Google Terms of Service ("TOS") and Privacy Policy in effect during the majority of the class period required users of Gmail to agree that "advertisements may be targeted to the content of information stored on [Google's] Services, queries made through [Google's] Services or other information."[3] (Declaration of Aaron Rothman (hereinafter "Rothman Declaration" or "Rothman Decl.") ¶ 11, Exh. E at § 17.1.) The Privacy Policy has essentially stated throughout the class period that Google could use information from users to "[p]rovide, maintain, protect, and improve [its] services (including advertising services) and develop new services." (*Id.* at ¶ 15, Exh. I; *see also id.* at ¶¶ 13-16, Exhs. G-J.)

In addition to these contractual terms, Google also provides a variety of disclosures throughout its website and within Gmail itself explaining that automated processing is applied to Gmail messages and that email content is scanned to deliver targeted ads. Several of these

[1] *See* Declaration of Kyle Wong (hereinafter "Wong Decl."), Exh. AA. In fact, attorneys for Plaintiff Dunbar filed a class action against Yahoo in this district claiming nearly identical allegations as brought here. (Compl. §§ 9-15 *Penkava v. Yahoo!, Inc.*, No. 12-cv-3414 PSG LHK (N.D. Cal.) ECF No. 1.) The case was subsequently dismissed with prejudice while Yahoo's motion to dismiss was pending. (*See* Wong Decl., Exh. PP.)

[2] *See, e.g.*, http://www.google.com/enterprise/apps/education/ and http://www.google.com/enterprise/apps/business/.

[3] The TOS defined Google's "Services" as "Google's products, software, services and web sites," including Gmail. (*See* Rothman Decl., Ex. F at §1.1.)

disclosures are detailed in the Rothman Declaration.

D. Plaintiffs, Their Consent to Automated Processing, and Their Claims.

Plaintiffs Dunbar, Fread, Carrillo, and J.K. (through A.K.) (collectively, "Gmail Plaintiffs") are Gmail or Google Apps users. (Compl. ¶¶ 224, 233, 345, 248.) Plaintiff Dunbar has a Google Apps account through his ISP, Cable One. Plaintiffs Fread and Carrillo have used Google Apps accounts provided by the universities they attend (Hawaii and UoP). J.K. is a minor who uses a Gmail account. These Gmail Plaintiffs claim that Google violated ECPA, 18 U.S.C. §§ 2511(1)(a) and (1)(d), by unlawfully intercepting and using their electronic communications. (*Id*. ¶ 216.) Each of these Gmail Plaintiffs are bound by the TOS, Privacy Policy, or both.[4]

Plaintiffs Brinkman, Knowles, and Brent Scott are residents of Pennsylvania, Maryland, and Florida respectively. They allege that they used their non-Gmail email accounts to communicate with Gmail users. (Compl. ¶¶ 10, 12, 13.) Based on these communications, these Plaintiffs claim that Google violated the state wiretap laws of their respective home states, Fla. Stat. §§ 934.03 *et seq*.; Md. Code, Cts. & Jud. Proc. §§ 10-402 *et seq*; 18 Pa. C.S. §§ 5701 *et seq*., by unlawfully intercepting and using their electronic communications (Compl. ¶¶ 332-384.) Because these states' wiretap laws are directly modeled on ECPA and are virtually identical to it in form and substance,[5] the claims of these Plaintiffs and the Gmail Plaintiffs (collectively, the "Wiretapping Plaintiffs") are considered and analyzed together below.

---

[4] Plaintiff Dunbar concedes that he is bound by the Cable One Apps TOS and Google's Privacy Policy. (Wong Decl., Exh. OO.) The relevant terms in the Cable One Apps TOS are virtually identical to, if not the same as, those terms in the Google TOS discussed above. (Rothman Decl. ¶ 7.) With respect to Plaintiffs Fread and Carrillo, as also discussed in the Rothman Declaration, the contracts between Google and Hawaii and UoP (i) incorporate the Privacy Policy, including its description of how Google processes data and (ii) require Hawaii and UoP to obtain the necessary consent from end users, like Fread and Carrillo, for Google to provide the Gmail service. (*Id*. ¶¶ 8 and 9, Exhs. C and D.) Plaintiff J.K. alleges that he created his Gmail account "via the 'Create An Account' link on Gmail's homepage." (Wong Decl., Exh. EE at ¶ 10.) As explained in the Rothman Declaration, a user who signs up in this manner must affirmatively agree to the TOS and Privacy Policy. (Rothman Decl. ¶ 6, Exh. A.) Moreover, at certain times during the class period, Google's Create an Account web page explained that in "Gmail, you won't see blinking banner ads. Instead, *we display ads you might find useful that are relevant to the content of your messages*." (*Id*. (emphasis added).) As such, each named Plaintiff is bound by the TOS, Privacy Policy, or both.

[5] *See, e.g.*, *Minotty v. Baudo*, 42 So. 3d 824 (Fla. Dist. Ct. App. 2010); *Deibler v. State*, 776 A.2d 657 (Md. Ct. App. 2001); *Kopko v. Miller*, 892 A.2d 766, 773 (Pa. 2006). As such, these statutes are to be construed in line with federal law under ECPA. *Minotty*, 42 So. 3d at 827; *Standiford v. Standiford*, 598 A.2d 495, 498 (Md. Ct. Spec. App. 1991); *Commonwealth v. Blystone*, 549 A.2d

Plaintiffs Brad Scott and Harrington, residents of Maryland and Alabama respectively, seek relief under California's Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630-632. These Plaintiffs (collectively, the "CIPA Plaintiffs") have non-Gmail email accounts through which they exchanged emails with Gmail users. Plaintiffs Brinkman, Knowles, Brent Scott, Brad Scott, and Harrington are referred to collectively as the "non-Gmail Plaintiffs."

While Plaintiffs seek to represent eight separate classes of Gmail and non-Gmail users under five causes of action, (Compl. ¶¶ 388-392), all Plaintiffs allege the same core theory of liability: that Google's automated scanning of emails is an illegal interception of their electronic communications without their consent. Plaintiffs claim that Google's systems "read[] each and every message" as part of the regular course of providing the Gmail service to its users. (*Id.* ¶ 3.) Plaintiffs purport to carve out spam filtering and virus detection from their claims, (*see, e.g.*, *id.* ¶¶ 43, 45), but their claims otherwise apply to *all* forms of scanning, regardless of the purpose or the benefits to Gmail users provided by scanning.

III. APPLICABLE STANDARDS.

This Motion is governed by Rule 12(b)(6) as interpreted in *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007) and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009). Under these standards, the court is "free to ignore legal conclusions, unsupported conclusions, unwarranted inferences and sweeping legal conclusions cast in the form of factual allegations." *Stanislaus Food Prods. Co. v. USS-POSCO Indus.*, 782 F. Supp. 2d 1059, 1064 (E.D. Cal. 2011); *see also Caviness v. Horizon Cmty. Learning Ctr., Inc.*, 590 F.3d 806, 812 (9th Cir. 2010).

IV. ARGUMENT

A. The Wiretapping Claims Fail Because the Alleged Scanning Practices Are Part of Google's Ordinary Course of Business as an ECS Provider.

1. The Wiretap Statutes Exempt ECS Providers from Liability.

The overall structure of ECPA[6] reflects Congress's careful effort to ensure that ECPA's

81 (Pa. 1988). For purposes of this motion, the only relevant difference between ECPA and these laws concerns their requirement of dual, as opposed to single, party consent, as discussed below.

[6] As background, ECPA "amended the Federal wiretap law" and was "divided into Title I, which governs unauthorized interceptions of electronic communications, 18 U.S.C. §§ 2510-2522, and Title II, which governs unauthorized access to stored communications, 18 U.S.C. §§ 2701-2711." *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 503 (2d Cir. 2005).

provisions regarding the "interception" of electronic communications will not interfere with ECS providers' ability to engage in their normal business practices. In enacting ECPA, Congress recognized that "provider[s] of electronic communications services may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain," and that such monitoring "may be necessary to the provision of an electronic communication service." (Wong Decl., Exh. BB [S. Rep. No. 99-541] at p. 20). With respect to email in particular, Congress noted that "the providers of electronic mail create electronic copies of private correspondence for later reference," and that "[t]his information *is processed for the benefit of the user*." *Id.* at 3 (emphasis added). *See also In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (explaining that emails must be "temporarily stored by electronic communications services incident to their transmission – for example, when an email service stores a message until the addressee downloads it").

Given these realities, Congress clarified that ECS providers can lawfully receive and access electronic communications involving their users–the very things that Plaintiffs contend are unlawful. For instance, while Section 2701 generally prohibits parties from accessing electronic communications in electronic storage, this provision "does not apply with respect to conduct authorized . . . by the . . . entity providing a wire or electronic communications service." 18 U.S.C. § 2701(c)(1). In other words, ECS providers are expressly authorized to access the communications sent to their systems. Title II prohibits ECS providers only from *disclosing* the electronic communications of their users, which is not at issue here (and even this general bar is subject to specific exceptions that allow an ECS provider to disclose communications in some circumstances). *See* 18 U.S.C. §§ 2701-2703.[7] *See, e.g., Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (Section 2701 "allows service providers to do as they wish when it comes to accessing communications"); *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 115 (3d Cir. 2003) (no ECPA liability under Section 2701 where ECS provider searched the contents of text messages in its systems).

[7] The state wiretapping statutes at issue include analogous terms. *See* Fla. Stat. §§ 934.21-23; Md. Code, Cts. & Jud. Proc. §§ 10-402 to -404; 18 Pa. C.S. §§ 5741-43; *see also* Appendix.

Similarly, Title I, relating to the interception of communications, contains several terms that exempt ECS providers from liability. Most importantly, Section 2510(5)(a)(i) excludes from the definition of "device" the equipment of an ECS provider used to access electronic communications "in the ordinary course of its business."[8] Thus, a "Wiretap Act claim requires, at a minimum, (a) an 'electronic communication' and (b) interception of that communication by someone *other than* 'a provider of wire or electronic communication service … in the normal course of' business . . . " *In re Google, Inc. Privacy Policy Litig.*, No. 12-cv-1382 PSG, 2012 WL 6738343, at *5 (N.D. Cal. Dec. 28. 2012) (emphasis added) ("*In re Google Privacy Policy*").

Other provisions further clarify that an ECS provider's normal practices are not an illegal "interception" under Section 2510. *See, e.g.*, 18 U.S.C. § 2511(2)(a)(i) (permitting employees and agents of an ECS provider "to intercept, disclose, or use" electronic communications being transmitted by the ECS for normal business purposes including "the protection of the rights or property of the" ECS provider); *id.* (permitting ECS providers to engage in "service observing" and "random monitoring" of electronic communications while prohibiting the same for wire (*e.g.*, telephone and telegraph) communications).

The rationale underlying these provisions is to ensure that ECS providers can deliver electronic communications and provide related services to their users without incurring liability under the provisions of the statute aimed at illicit behavior. As the Second Circuit explained in *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 505 (2d Cir. 2005), these provisions exempting ECS providers from liability must be applied consistently; otherwise, ECS providers "would constantly be intercepting communications under ECPA because their basic services involve the 'acquisition of the contents' of electronic communication."

2. Courts Have Consistently Dismissed Claims Against ECS Providers Involving Circumstances Similar to Those Alleged Here.

Applying this statutory scheme, courts have consistently rejected claims by plaintiffs attempting to characterize the normal business practices of ECS providers like Google as an illegal "interception" under the wiretapping statutes.

[8] The state wiretapping statutes at issue include analogous terms. *See* Fla. Stat. § 934.02(4)(a)2; Md. Code, Cts. & Jud. Proc. § 10-401(4)(i); 18 Pa. C.S. § 5702; *see also* Appendix.

For example, in *Kirch v. Embarq Management Co.*, 702 F.3d 1245 (10th Cir. 2012), the plaintiffs alleged that the defendant, an ISP, unlawfully "intercepted their Internet communications" by extracting information about their Internet browsing histories for the purpose of delivering targeted advertisements. *Id*. at 1245-48. The court affirmed the dismissal of the claim as a matter of law because all of the data at issue (plaintiffs' Internet browsing histories) was obtained in the course of defendant's business as an ISP. *Id*. at 1246, 1250-51. The fact that the ISP extracted a subset of the data for purposes of delivering targeted advertisements had no affect on the analysis "because [defendant's] access was in the ordinary course of its core business as an ISP transmitting data over its equipment." *Id*. at 1249. *See also id*. at 1250-51 (explaining that the advertising delivery system at issue "gave [the defendant] access to no more of [the plaintiffs'] electronic communications than it had in the ordinary course of its business as an ISP.").

Judge Grewal applied these same considerations to dismiss an ECPA claim in the specific context of a claim alleging that Google "intercepted" its users' information. In *In re Google Privacy Policy*, the plaintiffs alleged that "an interception occurred when their content from one Google product was . . . combined with information from another Google product that also was stored on Google's servers." 2012 WL 6738343, at *5-6. The claims in that matter were far broader than here; plaintiffs alleged that Google accesses and uses information from dozens of Google products, including Gmail, without consent to serve targeted advertisements and for other allegedly improper purposes. (Wong Decl., Exh. CC.) But as Judge Grewal recognized, even if Google's access and use of the information at issue exceeded the scope of Google's terms, there was no viable claim for an "interception" because "[a]n interception claim under the Wiretap Act also requires the use of a defined 'device,' *which cannot include Google's own systems . . .* " *In re Google Privacy Policy*, 2012 WL 6738343 at *5 (emphasis added). *See also id*. at *6 ("the inescapably plain language of [ECPA] . . . excludes from the definition of a 'device' a provider's own equipment used in the ordinary course of business."). Because the complaint did not allege the use of a "device" outside of Google's own systems, the Court dismissed the complaint as a matter of law. *Id*.

This case is no different. Plaintiffs' wiretapping claims fail because they do not allege the use of "a defined 'device'" distinct from "*Google's own systems*." *Id*. at *5 (emphasis added). Instead, the Complaint confirms that the alleged "interceptions" involve only Google's own equipment used in its capacity as an ECS provider. (*See* Compl., ¶¶ 22-92 (describing various Google servers and systems with no allegation of any non-Google device).) This alone mandates dismissal. *In re Google Privacy Policy*, 2012 WL 6738343 at *5.[9]

Moreover, the Complaint repeatedly confirms that the purpose of the alleged "interceptions" is to implement normal functions within the ordinary course of Google's business. Specifically, Plaintiffs complain that Google scans information from its users (the emails sent to and from Gmail users) in order to extract a subset of information (keywords and other information from the emails) "for the purpose of delivering content-based advertising."[10] (*See* Compl. ¶¶ 22-91, 259(g) (describing Google's processing of emails and alleging that Google does so to deliver advertising).) This is strikingly similar to the facts in *Kirch*, in which the defendant provided information from its users (their Internet activity) to a third party so that a subset of that information ("customer requests for highly trafficked commercial websites") could be used "to deliver online advertising thought likely to be interest users who visited those websites." 702 F.3d at 1247-48. As in *Kirch*, there is no illegal "interception" here because all of the email information at issue in Plaintiffs' claims stems from Google "access … in the ordinary course of its core business as [ECS provider] transmitting data over its equipment." *Id*. at 1249. Notably in *Kirch*, the defendant was accused, unlike here, of providing its users' information to a *third party*.

In short, there is no illegal "interception" here because Plaintiffs' own allegations confirm that the alleged practices at issue are part of Google's ordinary course of business.

3. Plaintiffs' Efforts to Plead around the "Ordinary Course of Business" Exemption Fail.

[9] *See also Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, No. 07-cv-1029, 2007 WL 4394447, at *4 (E.D. Pa Dec. 13, 2007) ("The drive or server on which an email is received does not constitute a device for purposes of the Wiretap Act.").

[10] Plaintiffs also note various other alleged purposes for Google's automated scanning, which further confirm that Google's practices are implemented for ordinary business reasons. (*See* Compl. ¶ 288 (alleging that Google scans emails for "commercial advantage and profits"); *id*. at ¶ 338 (alleging that Google scans emails to reduce certain "traffic acquisition costs").) Seeking profits and lowering costs are, of course, normal business purposes.

Rather than alleging any facts to show an illegal "interception," Plaintiffs seek to avoid the "ordinary course of business" exemption by claiming that Google's practices are not an "industry standard" practice. (Compl. ¶ 262.) Plaintiffs further suggest that Google's Gmail-related practices, including the delivery of targeted advertising, fall outside of the exemption because they are not a necessary "service of a provider of an electronic communication service." (Compl. ¶¶ 264-65.)

But the "ordinary course of business" exemption does not turn on whether an alleged practice is necessary for an ECS provider to deliver an electronic communication. Nor does the exemption turn on whether an ECS provider's practices conform to Plaintiffs' subjective notion of the prevailing "industry standard." Indeed, it would be nonsensical to assume that Congress intended to deprive an ECS provider of the "ordinary course of business" exemption simply because it chooses to run its business differently (or better) than its competitors.

Instead, the exemption applies broadly to protect an ECS provider's acts in the "course of *its* business." 18 U.S.C. 2510(5)(a)(ii)(emphasis added). For example, in *Hall*, the plaintiff argued that his email service provider did not act in the ordinary course of its business by continuing to deliver emails to customers who had terminated their accounts. 396 F.3d at 505. The Second Circuit did not inquire whether this practice was necessary to the defendant's business of delivering emails or whether it was consistent with prevailing industry standard. Instead, the Court applied the "ordinary course of business" exemption because it was the email service provider's *own* internal "practice at the time to continue to receive and store e-mails . . . after any account was cancelled." *Id*.

Similarly, the *In re Google Privacy Policy* plaintiffs alleged that Google's unique combination of products, including Gmail, allows it to target advertisements in a way that has no industry equivalent. (*See, e.g.*, Wong Exh. CC at ¶ 17 (alleging that Google's products, including Gmail, provide it with "targeted advertising capabilities" that "surpass those offered by social networks, such as Facebook.").) Yet these allegations did not deter Judge Grewal from applying the "ordinary course of business exemption," as discussed above. *In re Google Privacy Policy*, 2012 WL 6738343 at *5-6. In reaching that conclusion, the Court found no need to consider

whether Google's practices conform to an "industry standard" for the "services of an electronic communications service provider" (Compl. ¶¶ 262, 264-65), because those considerations are simply irrelevant.

The same result applies here: notwithstanding Plaintiffs' effort to plead around the "ordinary course of business" exemption, all wiretapping claims fail for the simple reason that the alleged conduct at issue is undisputedly part of *Google's* ordinary business practices as an ECS provider (and a provider of a free service at that).

4. Plaintiffs' Theory of Liability Would Lead to Absurd Results.

More generally, Plaintiffs' wiretapping claims should be rejected because they would criminalize an ECS provider's normal methods for processing emails and other electronic communications. Indeed, Plaintiffs' theory of liability—that the scanning of email content by an ECS provider is an illegal "interception"—directly conflicts with Title II, which expressly permits an ECS provider to "access" electronic communications sent to its systems (and even to disclose such communications in certain circumstances). The Court should not allow Plaintiffs to pursue a theory of an illegal "interception" that creates these sorts of irreconcilable conflicts within the statutory scheme. *See Hibbs v. Winn*, 542 U.S. 88, 101 (2004) ("A statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant.") (citation omitted); *Bayview Hunters Point Cmty. Advocates v. Metro. Transp. Comm'n*, 366 F.3d 692, 700 (9th Cir. 2004) (A statute "should not be interpreted in a way which is internally contradictory or that renders other provisions of the same statute inconsistent or meaningless.") (citation and quotation omitted).

In practice, Plaintiffs' theory would prevent ECS providers from providing a host of normal services that Congress could not possibly have intended to criminalize as an illegal "interception." For example, an ECS provider could not allow users to sort their emails using automated filters because any such system would require scanning the contents of the emails being delivered to the user, thus running afoul of Plaintiffs' theory. Nor could an ECS provider provide even basic features like allowing users to search their own emails for particular key terms because doing so would, again, involve the scanning of email content. And while Plaintiffs have

removed spam filtering and virus detection from their claims, these selective carve-outs simply underscore the fact that their sweeping theory of liability would *otherwise* encompass these basic (and desirable) features of email.[11]

In short, Plaintiffs' interpretation would render large swaths of the statutory scheme meaningless while making it virtually impossible for ECS providers to provide normal services to their users. The Court should not allow Plaintiffs to proceed on this basis.

5. The Pennsylvania Wiretap Statute Applies Only to the Senders, Not the Recipients of a Communication.

A further basis exists under Pennsylvania law to reject Plaintiff Brinkman's claim of an alleged "interception." Section 5725 of the Pennsylvania statute only authorizes a private right of action for a person "whose wire, electronic or oral communication is intercepted, disclosed or used . . . " 18 Pa. C.S. § 5725. Pennsylvania courts have interpreted this to mean "that the cause of action belongs to the person with whom the communication originated, not the recipient." *Klump v. Nazareth Area Sch. Dist.*, 425 F. Supp. 2d 622, 633 (E.D. Pa. 2006) (citing *Kline v. Sec. Guards, Inc.*, 386 F.3d 246, 257 (3d Cir. 2004)). In *Klump*, the plaintiff lacked standing under section 5725 because the allegedly intercepted communications were sent *to* him, and therefore he could not meet the first requirement of the prima facie case. *Id.* at 633. To the extent that Plaintiff Brinkman seeks to bring claims for emails that she received but did not author (Compl. §§ 365, 391), she has no private right of action and her claim must be dismissed. *Id.*

B. Plaintiffs' Claims Also Fail Under the Consent Defenses of the Wiretap Statutes at Issue.

In addition to the lack of any illegal "interception," the Wiretapping Plaintiffs' claims also fail for the additional reason that the senders and recipients of the emails at issue have all

[11] The wiretapping claims of Plaintiffs Fread and Carrillo are further undermined by the Family Educational Rights and Privacy Act of 1974 ("FERPA"). Plaintiffs Fread and Carrillo allege that Google violated the Wiretap Act by processing their emails on behalf of the universities at which they are enrolled. But Plaintiffs admit that Google's actions were taken under contracts with each university, in which the university outsourced its email processing to Google. Even assuming, arguendo, that FERPA applies here, the law permits schools to "outsource[] institutional services or functions," including provision of email services. *See* 34 C.F.R. 99.31(a)(1)(i)(B). A party such as Google, to whom this function has been outsourced, is deemed a "school official," and as such may access and use student records, even without student consent. *Id.* The Court should not construe an "interception" under the Wiretap Act in a manner that would criminalize conduct that is expressly permitted under FERPA and its implementing regulations.

necessarily consented to the processing of their emails by Google.

The consent defense to a wiretap claim can be based on the terms of an express agreement. *See, e.g., Smith v. Trusted Universal Standards in Elec. Transactions, Inc.*, No. 09-cv-4567, 2011 WL 900096, at *10-11 (D.N.J. Mar. 15, 2011) ("[B]y subscribing to [Microsoft's email service], each Microsoft customer consents to Microsoft intercepting and filtering all of his email communications."). Consent can also be implied from the overall circumstances of a particular communication. *See, e.g., United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996) (consent may be "implied in fact from surrounding circumstances . . . ") (citation and quotation omitted).

Under federal law, the consent of a *single* party to a communication is complete defense to any liability and so the consent of the Gmail user alone is sufficient to bar a claim. *See* 18 U.S.C. § 2511(2)(d). The state wiretap statutes at issue also provide a defense where both parties to the communication consent to the alleged interception. Fla. Stat. § 934.03(2)(d); Md. Code, Cts. & Jud. Proc. § 10-402(c)(3); 18 Pa. C.S. § 5704(4).

1. The Gmail Plaintiffs Expressly Consent to Automated Scanning, Precluding Any Claim under ECPA.

The single-party consent defense under federal law precludes the Gmail Plaintiffs' claims as a matter of law because they expressly consented to automated scanning in exchange for using the free Gmail service. The Gmail Plaintiffs concede that by signing up for, or using, their Gmail or Google Apps accounts (Compl. ¶¶ 219, 223, 233, 241, 247), they are contractually bound to Google's terms. Indeed, they devote much of the Complaint to attacking the disclosures in the TOS and Privacy Policy in an effort to avoid this express contractual consent.

Because the Gmail Plaintiffs are bound to Google's TOS and/or Privacy Policy, they have expressly consented to the scanning disclosed in these terms. For example, the TOS in effect during the majority of the proposed class period informed users that Google's services, including Gmail, are supported by advertising revenue and that Google may display advertising targeted to the content of user information, including emails in Gmail accounts: "[A]dvertisements may be

targeted to the content of information stored on the Service[12], queries made through the Service or other information." (Rothman Decl., ¶ 11, Exh. E, at § 17.1.) This TOS further provided that "Google reserves the right . . . to pre-screen, review, flag, filter . . . any or all Content from any Service." (*Id.* at § 8.3.) The Google Privacy Policies throughout the class period declared in varying but clear terms that Google may use the information from users to "[p]rovide, maintain, protect, and improve our services (including advertising services) and develop new services." (*Id.*, ¶ 16, Exh. I; *see also id.* ¶¶ 13-16, Exhs. G-J.)

Google updated its TOS and Privacy Policy on March 1, 2012. These updated versions (which are currently in effect, but for an unrelated change in the Privacy Policy in July 2012) also explained, and required users to agree to, the automated scanning practices at issue. The updated TOS notifies users that "Google's privacy policies explain how we treat your personal data and protect your privacy," and that "[b]y using our Services, you agree that Google can use such data in accordance with our privacy policies." (*Id.*, ¶ 12, Exh. F.) The updated Privacy Policy, in turn, explains that Google collects information that users generate while using Google's services, including Gmail, and can use information from "all of [Google's] services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and [its] users." (*Id.* ¶ 16, Exh. J.) The Privacy Policy further specifies that Google "also use[s] this information to offer you tailored content – like giving you more relevant search results and ads." (*Id.*)

These express terms plainly encompass Google's scanning of email content as part of providing the Gmail service. Because the Gmail Plaintiffs are bound to these terms as a condition of using Gmail[13], they cannot pursue a claim under ECPA, which precludes liability based on a single party's consent. *Kirch v. Embarq Mgmt. Co.*, No. 10-cv-2047, 2011 WL 3651359, at *7-8 (D. Kan. Aug. 19, 2011) (finding consent based on defendant's terms of service); *Deering v. CenturyTel, Inc.*, No. 10-cv-0063, 2011 WL 1842859, at *1-3 (D. Mont. May 16, 2011)

[12] "Services" is a defined term that includes broadly covers all Google services, including Gmail. (*See* Rothman Decl., Ex. E at §1.1.)

[13] As referenced in note 4, the Cable One Apps TOS that Plaintiff Dunbar agreed to includes essentially identical terms as the Google TOS referenced above (with minor differences as noted in the Rothman Declaration) and links to the same Google Privacy Policy. Further, Hawaii and UoP were contractually required to obtain the necessary consent from end users, like Fread and Carrillo, for Google to provide the Gmail service.

(dismissing ECPA against ISP based on users' consent to privacy policy).[14]

2. Minors like Plaintiff J.K. Cannot Avoid the Terms They Agreed To.

Trying to wriggle free from these binding terms, Plaintiff J.K. (one of the Gmail Plaintiffs) claims he "could not have consented" because he is sixteen years old and his agreement is thus "void" under California law. (Compl. ¶¶ 250, 275.) To support this assertion, Plaintiff J.K. relies principally on Section 6701(c)[15] of the Family Code, which provides that contracts with minors are void if they "relat[e] to any personal property not in the immediate possession or control of the minor." Cal. Fam. Code § 6701(c). But there is nothing in the Family Code or any authority applying the statute suggesting that an agreement in which a minor provides consent to the use of his information is a contract concerning "personal property." *Compare Taylor v. Indus. Accident Comm'n*, 216 Cal. App. 2d 466, 473 (1963) (applying the predecessor statute to Section 6701 with identical terms and holding that hard copies of newspapers are "personal property"). Moreover, Plaintiff J.K.'s express consent to the automated processing of his emails cannot fall within the scope of Section 6701(c) because Plaintiff's emails *are* "within [his] possession or control." Like all Gmail users, Plaintiff J.K. is in full control of the emails in his Gmail account and can select what emails to send, which emails to retain, and which to delete. Under these circumstances, the contractual consent that Plaintiff J.K. gave to Google does not fall within either the terms or the underlying purpose of Section 6701(c).

Even if the California Family Code could be construed to invalidate Plaintiff J.K.'s

[14] *See also Mortensen v. Bresnan Commc'n, LLC*, No. 10-cv-0013, 2010 WL 5140454, at *3-5 (D. Mont. Dec. 13, 2010) (dismissing ECPA claim against ISP based on its users' consent in the account agreement, privacy policy, and other posted notices); *In re Vistaprint Corp. Mktg. & Sales Pracs. Litig.*, No. 08-md-1994, 2009 WL 2884727, at *9 (S.D. Tex, Aug. 31, 2009), *aff'd*, 392 F. App'x 327 (5th Cir. 2010) (dismissing ECPA claim based on consent); *Borninski v. Williamson*, No. 02-cv-1014, 2005 WL 1206872, at *12-13 (N.D. Tex. May 17, 2005) (no ECPA violation where plaintiff signed agreement and expressly consented to defendant's monitoring of his communications).

[15] The Complaint also refers in passing to Section 6701(a), which provide that contracts with minors are deemed void if they involve a "delegation of power." (Compl. ¶ 274.) But apart from parroting the statutory term, Plaintiffs allege no facts to show how Google's terms could fall within this provision. In addition to these categories of void contracts, California law also allows minors to disaffirm an otherwise enforceable contract in limited circumstances under Section 6710. Plaintiff J.K., however, does not specify that he seeks to disaffirm his contract under this provision and asserts only that his agreement is void under Section 6701. *See Berg v. Traylor*, 148 Cal. App. 4th 809, 820 (2007) (a minor's disaffirmance must be reflected in an "unequivocal intent to repudiate [the contract's] binding force and effect.") (citation and quotation omitted).

express consent, it would be preempted by the federal Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-08. COPPA reflects Congress's judgment that operators of websites *can* obtain and use information from teens like Plaintiff J.K. by obtaining their consent. Under COPPA, an "operator of a website or online service" cannot deal directly with a minor and must obtain parental consent in order to "collect" or "use" the "personal information" of a "child"—but *only where the child is "under the age of 13."* *Id.* §§ 6501(1), 6502(a)(1), (b)(1)(A). In enacting these terms, Congress specifically considered *and rejected* a parental consent requirement for teens like Plaintiff J.K. (*See* Wong Decl., Exh. JJ [the "COPPA FAQ"], No. 11] ("In enacting [COPPA], Congress determined to apply the statute's protections only to children under 13").)

Rather than requiring parental consent, the regulatory scheme of COPPA encourages websites to obtain consent directly from teens in connection with the use of their information. As the Federal Trade Commission ("FTC") explains in its COPPA FAQ: "Although COPPA does not apply to teenagers, the FTC is concerned about teen privacy and does believe that strong, more flexible, protections may be appropriate for this age group." (*Id.*) To illustrate these alternative "protections" for teens, the COPPA FAQs refer to a separate FTC Report that encourages websites to obtain "affirmative express consent" from teens in certain circumstances (while emphasizing that consent "may not be necessary in every advertising campaign directed to teens"). (*See* Wong Decl., Exh KK). To ensure consistent application of these standards, COPPA expressly preempts any state law that treats the use of "personal information" in a manner that "inconsistent" with COPPA. *See* 15 U.S.C. § 6502(d).

This federal statutory scheme bars Plaintiff J.K. from using the California Family Code to invalidate the "affirmative express consent" that he gave to Google—consent that Google was not only allowed to obtain but *encouraged* to obtain from Plaintiff J.K. under COPPA.

3. Plaintiffs Fread and Carrillo Cannot Avoid Their Express Consent by Claiming They Were Pressured into Using Gmail.

Nor can Plaintiffs Fread and Carrillo avoid Google's terms merely by suggesting that they felt pressured to use their university email accounts operated through Google Apps. For example,

Fread alleges that he initially avoided using his email account knowing it would be processed similarly to Gmail, but was forced to acquiesce "in order to send and receive official [university] communications." (Compl. ¶ 233.) Plaintiff Carrillo similarly claims he used his university account due only to a "forced migration process," although he concedes he clicked to agree to the "terms and conditions" and "privacy policy" associated with the new account. (*Id.* ¶ 241.)

These vague assertions do nothing to undermine the enforceability of the terms that are binding on these Plaintiffs. Under California law, a party may avoid a contract under a claim of duress only if it can show that "a party intentionally used threats or pressure to induce action or nonaction to the other party's detriment" where "[t]he coercion . . . induce[d] the assent of the coerced party, who has no reasonable alternative to succumbing." *In re Marriage of Baltins*, 212 Cal. App. 3d 66, 84 (1989) (citing Restatement (Second) of Contracts § 175(1)(1981)) (other citations and internal quotation omitted). While these Plaintiffs suggest they felt pressured by circumstances to use their email accounts, they do they not allege that this pressure was due to any "threats or coercion" by Google or that they lacked "a reasonable alternative," as would be needed to invalidate their express contractual consent under state law. Moreover, courts have held that the continued use of a form of communication that an individual knows may be monitored or recorded is sufficient to supply consent under the Wiretap Act–*even if* there was no meaningful choice. *See, e.g.*, *United States v. Verdin-Garcia*, 516 F.3d 884, 894 (10th Cir. 2008) ("A prisoner's voluntarily made choice—even a Hobson's choice—to use a telephone he knows may be monitored implies his consent to be monitored.").

Accordingly, Plaintiffs Fread's and Carrillo's individual allegations are irrelevant as a matter of law and do not undermine the express consent they gave.[16]

[16] As a separate basis for avoiding express consent, Plaintiffs make a vague reference to Section 2511(2)(d), which provides that the consent defense is inapplicable where a communication is "intercepted for the purpose of committing any criminal or tortious act . . . " (Compl. ¶ 281.) This provision applies only where the defendant acted with a specific intent to cause injury. *See, e.g.*, *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 515 (discussing Section 2511(2)(d) at length and noting congressional intent to invalidate consent only where "the party acts in any way with an intent to injure the other party") (emphasis omitted). Here, the Complaint is devoid of a single allegation to show that Google had the specific intent to harm its Gmail users.

4. The Non-Gmail Plaintiffs Also Impliedly Consent to the Automated Processing of Their Messages.

The state law wiretap claims of the Non-Gmail Plaintiffs fail for similar reasons. While the non-Gmail Plaintiffs are not bound to Google's contractual terms, they nonetheless impliedly consent to Google's practices by virtue of the fact that *all* users of email must necessarily expect that their emails will be subject to automated processing.

Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use web-based email today cannot be surprised if their communications are processed by the recipient's ECS provider in the course of delivery. Indeed, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). In particular, the Court noted that persons communicating through a service provided by an intermediary (in the *Smith* case, a telephone call routed through a telephone company) must necessarily expect that the communication will be subject to the intermediary's systems. For example, the Court explained that in using the telephone, a person "voluntarily convey[s] numerical information to the telephone company and 'expose[s]' that information to its equipment *in the ordinary course of business*." *Id*. at 744 (emphasis added).

The same is true of email sent through an ECS provider. As numerous courts have held, the automated processing of email is so widely understood and accepted that the act of sending an email constitutes implied consent to automated processing as a matter of law. *See, e.g., State v. Townsend*, 57 P.3d 255, 260 (Wash. 2002) (finding that sender of email impliedly consented to interception of his email because "in order for e-mail to be useful it must be" subjected to automated processes, such as being "recorded on another computer's memory."); *Commonwealth v. Proetto*, 771 A.2d 823, 829 (Pa. Super. Ct. 2001), *aff'd*, 837 A.2d 1163 (Pa. 2003) ("Any reasonably intelligent person, savvy enough to be using the Internet, however, would be aware of the fact that messages are received in a recorded format, by their very nature, and can be downloaded or printed by the party receiving the message. By the very act of sending a communication over the Internet, the party expressly consents to the recording of the message.");

State v. Lott, 879 A.2d 1167, 1172 (N.H. 2005) (sender of instant messages "implicitly consented" to the interception of his communications where he voluntarily sent instant messages knowing that, by the medium's nature, his messages would be automatically recorded).[17]

Similarly here, non-Gmail users who send emails to Gmail recipients must expect that their emails will be subjected to Google's normal processes as the ECS provider for their intended recipients. Indeed, when the non-Gmail Plaintiffs filed their initial complaints, some specifically alleged that they *continued to send emails to Gmail users* despite their knowledge of Google's automated scanning (as confirmed in their complaints).[18] This ongoing use shows that Google's automated scanning was completely immaterial to these Plaintiffs' decisions to communicate with Gmail users and suggests that they were aware of Google's automated scanning all along. In fact, Plaintiff Fread's own allegations confirm that Google's automated scanning is common knowledge among non-Gmail users. Plaintiff Fread alleges he spent months trying to avoid using his Google Apps account, due to his awareness of and apparent concern about Google's email processing. (Compl. ¶ 233.) So too, the non-Gmail Plaintiffs must have expected that their emails to Gmail recipients would be subject to automated processing by Google in its capacity as the ECS provider for their intended recipients. As in *Smith*, these Plaintiffs cannot claim ignorance because they "voluntarily conveyed" emails to Google as an ECS provider and "'expose[d]' that information to [Google's] equipment in the ordinary course of business." 442 U.S. at 744. Under these circumstances, the non-Gmail Plaintiffs have impliedly consented to Google's automated scanning. Thus, in combination with the express consent of the Gmail recipients (as discussed above), their communications are subject to the dual-party consent defenses of the state wiretapping laws and their claims must be dismissed as a matter of law.

---

[17] *See also State v. Roden*, 279 P.3d 461, 466 (Wash. Ct. App. 2012) (finding that the defendant "impliedly consented" to a law enforcement officer's interception of his text messages because "as a user of text message technology," the defendant necessarily "understood that [his drug dealer's cell phone] would record and store the text messages that he sent"); *Commonwealth v. Maccini*, No. 06-cv-0873, 2007 WL 1203560, at *3 (Mass. Super. Ct. Apr. 23, 2007) (holding that, given the nature of email communications, law enforcement's "receipt and recording of the defendant's communications was not secret but rather was *with the defendant's knowledge and implicit consent*." (emphasis added)).

[18] *See* Wong. Decl., Exh. EE (J.K. Compl. ¶ 21); Exh. FF (Knowles Compl. ¶ 20); Exh. GG (Brinkman Compl. ¶ 15); Exh. II (Scott II Compl. ¶ 15).

In sum, the Wiretapping Plaintiffs' claims fail in their entirety due to both the "ordinary course of business" exemption and the consent defenses applicable under ECPA and the state wiretapping statutes at issue.[19]

C. The CIPA Claim Also Fails as a Matter of Law for Multiple Reasons.

1. CIPA Does Not Apply to Email Communications.

The CIPA claim fares no better because the statute, enacted in 1967, was never intended to apply, and by its terms cannot be applied, to emails. On its face, Section 631 of CIPA is limited to interceptions that involve "telephone and telegraph" communications. *See* Cal. Penal Code § 631.[20] The first clause of Section 631 expressly refers to wiretapping of a "*telegraph* or *telephone wire, line, cable, or instrument*." *Id.* (emphasis added). The second clause covers other forms of interception that involve "read[ing]" or "learn[ing] the contents" of a communication, but reiterates that liability only applies if the communication is "in transit or passing over *any wire, line, or cable*, or is being sent from, or received at any place within this state." *Id.* (emphasis added). While the term "telegraph or telephone" is not repeated in the second clause, it would be nonsensical to assume that the Legislature intended to cover two totally different categories of "wire[s], line[s], or cable[s]" in two clauses of the same single-sentence provision. For this reason, California courts have interpreted Section 631 as focusing on telephone and telegraph communications alone. *See People v. Chavez*, 44 Cal. App. 4th 1144, 1150 (1996) (explaining that "[w]iretapping refers to the interception by any method of *telegraphic or telephonic communications*") (emphasis added).

Section 632 similarly excludes electronic communications. In particular, Section 632 is targeted at "[e]avesdropping." *See* Cal. Penal Code § 632. Obviously, one cannot "eavesdrop" on an email or other purely electronic communication in any normal sense of the word. *See*

---

[19] These same considerations apply to the Gmail Plaintiffs and CIPA Plaintiffs as well. As to the Gmail Plaintiffs, even if the Court does not find express contractual consent as to the Gmail Plaintiffs, their claims would be barred based on implied consent given their continuing use of their Gmail accounts, even after discovering Google's alleged scanning of their emails. *See* note 18, *supra*. Also, CIPA provides for a defense based on consent and should be dismissed on this basis, in addition to the CIPA-specific reasons set forth herein. *See* Cal. Penal Code §§ 631-632.

[20] The full text of Sections 631 and 632 are set forth in the attached Appendix of Relevant Statutes for the court's convenience.

Black's Law Dictionary, 588 (9th ed. 2009) (defining "eavesdropping" as "[t]he act of secretly listening to the private conversation of others without their consent."). While Section 632 also refers to the "record[ing]" of confidential communications, that reference must be interpreted consistently with the overall statute, which plainly focuses on oral communications. *See* Cal. Penal Code § 632.

Construing these terms, a California court has specifically held that ***CIPA does not apply to the automated processing of emails in the Gmail system***. In *Diamond v. Google Inc.*, No. CIV-1202715, the Marin County Superior Court dismissed the Section 632 claim because the plaintiff had not explained "how Google could have possibly 'overheard' the emails 'by means of any electronic amplifying or recording device'" for purposes of the statute. The court also held that Section 631 cannot be expanded beyond its express limitations to telephone and telegraph equipment, explaining that "the words 'telegraph or telephone' … can only be reasonably construed to apply to" Section 631 as a whole. (*See* Wong Decl., Exh. LL at p. 2.) The court thus dismissed the Section 631 claim because "Plaintiff allege[d] no facts allowing email communications to be characterized as 'telephone' or 'telegraph' transmissions." (*Id.*) The same common sense analysis should be applied here.

Indeed, any contrary interpretation of CIPA as encompassing emails would be nonsensical because the Legislature could not possibly have contemplated email when it enacted the statute in 1967. As the Supreme Court has long cautioned, "[i]t is not the function of the judiciary, because of discoveries after the [initial enactment of a statute], to broaden the provisions of that act so that it will include corporations or companies that were not, and could not have been at that time, within the contemplation of Congress." *City of Richmond v. S. Bell Tel. & Tel. Co.*, 174 U.S. 761, 774-776 (1899) (holding that statute applying to "telegraph lines" could not be applied to telephone technology implemented after the statute's enactment).[21] Plaintiffs' claims violate this

[21] *See also State v. Komisarjevsky*, No. CR07241860, 2011 WL 1032111, at *3 (Conn. Super. Ct. Feb. 22, 2011) (News reports sent via Twitter do not fall within a rule related to "broadcasting" because the rule predated Twitter and "[c]ourts traditionally have proceeded with caution in extending old legislation to new technologies.") (citation omitted); *Deacon v. Pandora Media, Inc.*, 901 F. Supp. 2d 1166, 1172-75 (N.D. Cal. 2012) (statutory terms related to "selling," "renting" and "lending" music could not be applied to online music streaming because streaming technology could not have been contemplated at the time of the statute's enactment).

basic rule by rewriting CIPA to encompass email technology that simply did not exist when the statute was enacted.

In fact, after CIPA's initial enactment, ***the Legislature specifically considered and rejected proposals to expand the statute to cover emails***. In 1995, the Legislature expanded Penal Code Section 629 (a related statute to CIPA that regulates interception of communications by law enforcement) to cover certain types of electronic communications. In considering the bill, the Senate Judiciary Committee observed that "[i]t is not clear that California law specifically protects e-mail and other electronic communications from improper interception by either private parties or law enforcement." (Wong Decl., Exh. MM at p. 4.) It thus posed the question "SHOULD, AS A COROLLARY TO THE EXTENSION OF THE WIRETAP LAW [Section 629] TO ELECTRONIC COMMUNICATIONS, THE PRIVACY LAWS [CIPA] BE AMENDED TO EXPRESSLY PROTECT ELECTRONIC COMMUNICATIONS FROM INTERCEPTION …." (*Id.* at 4 (caps in original).) Ultimately, the Legislature opted to amend *only* Section 629 while declining to expand CIPA in similar fashion. (*Id.*)

In 2010, Section 629 was expanded again to cover additional forms of electronic communications. As the Senate Committee on Public Safety explained, the language of Section 629 at the time—which was already *broader* than CIPA—still did not cover emails and other forms of electronic communications. (*See* Wong Decl. Exh. NN (Senate Analysis stating that "[t]his bill … updates California's wiretapping law to include interception of communications by e-mail, blackberry, instant messaging by phone and other forms of contemporaneous two way electronic communication.").) Again, the Legislature decided to amend *only* Section 629, leaving the limitations of Sections 631 and 632 intact.

In sum, the express terms of the statute, the applicable rules of statutory interpretation, and legislative history all confirm that CIPA does not reach email communications.

2. Plaintiffs Also Have No Article III Standing to Pursue a CIPA Claim.

The CIPA Plaintiffs' claim also fails for an additional and equally fundamental reason: they allege no facts to show they suffered an injury-in-fact sufficient to confer standing under

Article III of the Constitution.[22] While Ninth Circuit authority may be read to permit standing based on the violation of certain statutory rights without independent allegations of harm, this applies *only* to statutes that specifically allow persons who meet the express statutory criteria to bring a claim without any showing of injury. *In re iPhone Application Litig.*, No. 11-md-2250, 2011 WL 4403963, at *6 (N.D. Cal. Sept. 20, 2011) (finding that plaintiffs had no Article III standing because they "do not allege a violation of [a] statute which does not require a showing of injury."). In contrast, CIPA expressly provides that a civil claim can be brought only by a "*person who has been injured.*" Cal. Penal Code § 637.2 (emphasis added). Accordingly, Plaintiffs cannot pursue a CIPA claim without establishing the standing requirements of both CIPA and Article III.

Here, the CIPA Plaintiffs fail to allege any concrete injury stemming from the automated processing of the emails they sent to the Gmail system. While they vaguely assert that Google improperly used information contained in their emails, this Court has held that merely alleging the "collection and tracking of . . . personal information" is insufficient to confer standing under Article III. *See In re iPhone Application Litig.*, 2011 WL 4403963, at *5; *see also LaCourt v Specific Media, Inc.*, No. 10-cv-1256, 2011 WL 1661532, at *3-4 (C.D. Cal. Apr. 28, 2011) (plaintiffs had no Article III standing to bring claims involving use of Flash cookies to track Internet activity). Plaintiffs' allegations here are no different, and their CIPA claim similarly fails for lack of Article III standing.

3. Plaintiffs Also Fail to Allege Any Connection with California.

In addition to alleging injury, the CIPA Plaintiffs must also show that their communications have some contact with California. Section 631 specifically regulates the interception of communications "while the same [are] in transit or passing over any wire, line, or cable, or [are] being sent from, or received at *any place within this state*." Cal. Penal Code § 631(a) (emphasis added). This same limitation applies to Section 632. *See Kearney v. Salomon*

[22] Under Article III, "a plaintiff must show (1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000).

Smith Barney, Inc., 39 Cal. 4th 95, 119 (2006) (explaining that Section 632 "protect[s] against the secret recording of any confidential communication that is sent from or received *at any place within California*.") (emphasis added). Here, the CIPA Plaintiffs (who reside in Alabama and Maryland) do not allege that any of their emails have any connection to California. For example, they make no effort to allege that they ever sent a single email to a recipient in California, even though that information is obviously within their knowledge. The CIPA claims of these Plaintiffs should be dismissed given this basic failure of pleading.

D. The Section 632 Claim Fails for Additional Reasons.

1. Plaintiffs Allege no Facts to Show that Their Emails Were "Confidential Communications" within the Meaning of the Statute.

Section 632 applies only to "confidential communication[s]," defined as communications made "in circumstances" that "reasonably indicate" a "desire[]" that the communications "be confined to the parties thereto." Cal. Penal Code § 632(c). This definition excludes communications made "in any . . . circumstance in which the parties . . . may reasonably expect that the communication may be overheard or recorded." *Id.* Applying this requirement, courts have consistently dismissed Section 632 claims where plaintiffs allege that they subjectively expected their communications to be confidential, without pleading additional facts to demonstrate that the communication falls within the scope of Section 632. *See, e.g., Faulkner v. ADT Servs., Inc.*, 706 F.3d 1017, 1021 (9th Cir. 2013) (affirming dismissal of Section 632 claim where plaintiff alleged that he expected his communication to be confined to the parties, but did not allege sufficient facts to show he had an "objectively reasonable" expectation that the communication would not be recorded).[23]

Similarly here, the CIPA Plaintiffs claim they had no "knowledge or expectation" that the emails they sent to Gmail users would be processed by Google. (Compl. at ¶ 316.) But beyond

[23] *See also Montegna v. Yodle, Inc.*, No. 12-cv-0647, 2012 WL 3069969, at *3 (S.D. Cal. July 27, 2012)(dismissing Section 632 claim where plaintiff alleged recording of a "confidential" conversations but failed "to allege any facts regarding [the plaintiffs'] relationship with [the other parties to the communication]" or "the content or nature of the calls."); *Weiner v. ARS Nat'l Servs., Inc.*, 887 F. Supp. 2d 1029, 1033 (S.D. Cal. 2012) (dismissing Section 632 claim where plaintiff failed to allege the relationship between the parties to the communication, or that the communication contained any "personal information.")

those conclusory assertions, they plead no actual facts to show their emails were sent under "circumstances" that would "reasonably indicate" a "desire[]" that the emails "be confined to the parties." *See* Cal. Penal Code § 632(c). Among other omitted facts, the CIPA Plaintiffs do not describe the content or nature of a single email they sent to a Gmail user[24]; nor do they describe their prior experiences with email services to suggest any basis for their expectations.[25] As in *Faulkner*, "too little is asserted in the complaint about the particular relationship between the parties, and the particular circumstances of the [communications at issue], to lead to the plausible conclusion that an objectively reasonable expectation of confidentiality would have attended such a communication." 706 F.3d at 1020.

2. Federal Law Preempts Any Claim that an ECS Provider's Operations Constitute an Illegal "Recording" under Section 632.

As set forth above, ECPA set forth a comprehensive scheme related to ECS providers, which allows providers of email services like Google to "store" and "access" emails sent to its systems. In enacting these provisions, Congress expressed specific concern that conflicting state standards could "discourage potential customers from using innovative communications systems" and "discourage [ECSs and Remote Computing Services ("RCS")] from developing new innovative forms of telecommunications and computer technology." (Wong Decl., Exh. BB at p. 5.) Reflecting these legislative concerns, courts have found that ECPA preempts overlapping state law regulations of electronic communications. *See In re Google, Inc. Street View Elec. Commc'ns Litig.*, 794 F. Supp. 2d 1067, 1084-85 (N.D. Cal. 2011) (holding that ECPA preempts state wiretap statutes because the statute "comprehensively regulate[s] the interception of electronic communications such that the scheme leaves no room in which the states may further regulate."); *Bunnell v. MPAA*, 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2007) (ECPA preempts CIPA claim regarding access to emails).

Under these standards, Plaintiffs cannot seek to impose liability on Google for "recording"

[24] For example, there could be no reasonable expectation of confidentiality if the CIPA Plaintiffs' emails with Gmail users were sent to large groups of recipients or were sent with the express expectation that they would be forwarded to others, among other circumstances that would preclude application of Section 632.

[25] For example, if Plaintiffs used Yahoo mail, they would have known that automated scanning of emails to deliver advertising is a common industry practice not limited to Gmail. *See* n.11, *supra*.

the emails that are sent to Gmail recipients because ECPA specifically allows Google to receive and store electronic such communications in its capacity as an ECS provider. Even if CIPA could be interpreted to apply to emails at all, Plaintiffs' Section 632 claim based on Google's "recording" of emails is preempted as a matter of law because it is in direct conflict with federal law.[26] *See Ting v. AT&T*, 319 F.3d 1126, 1137 (9th Cir. 2003) ("Even where Congress has not entirely displaced state regulation in a specific area, state law is preempted to the extent that it actually conflicts with federal law."); *Pub. Util. Dist. No. 1 v. IDACORP, Inc.*, 379 F.3d 641, 650 (9th Cir. 2004) ("Under the obstruction strand of conflict preemption, an aberrant or hostile state rule is preempted to the extent it actually interferes with the methods by which the federal statute was designed to reach [its] goal.").

E. The CIPA Claim Should Also be Dismissed under Choice of Law Principles.

Apart from the various defects above, choice-of-law principles preclude the CIPA Plaintiffs—as residents of Alabama and Maryland—from invoking CIPA and bypassing the law of their local jurisdictions.[27] Under the "governmental interest" analysis[28], (1) a court "determines whether the relevant law of each of the potentially affected jurisdictions" differ, (2) "if there is a difference, the court examines each jurisdiction's interest in the application of its own law . . . to determine whether a true conflict exists," and (3) if a true conflict exists, the court must weigh "the interest of each jurisdiction in the application of its own law to determine which state's interest would be more impaired if its policy were subordinated to the policy of the other state . . . " *Mazza*, 666 F.3d at 590. These standards mandate application of Alabama and Maryland law here.

---

[26] Plaintiffs also refer in conclusory terms to the "eavesdropping" element of Section 632, but cannot seriously contend that the automated processing of emails by computer systems amounts to "eavesdropping" on a communication.

[27] Choice of law determinations in class actions are routinely resolved at the pleading stage. *See, e.g., Frezza v. Google, Inc.*, No. 12-cv-0237, 2013 WL 1736788, at *5 (N.D. Cal. Apr. 22, 2013) (stating that *Mazza v. Am. Honda Motor Co., Inc.*, 666 F.3d 581 (9th Cir. 2012) was "not only relevant but controlling" and dismissing UCL claims because North Carolina law applied); *Banks v. Nissan N. Am., Inc.*, No. 11-cv-2022, 2012 U.S. Dist. LEXIS 37754, at *3 (N.D. Cal. Mar. 20, 2012) (dismissing nationwide class action claim predicated on California law because "such allegations are inappropriate, pursuant to the Ninth Circuit's reasoning in *Mazza* . . . ").

[28] "A federal court sitting in diversity must look to the forum state's choice of law rules to determine the controlling substantive law." *Mazza*, 666 F.3d 589-90 (citation omitted).

The potentially applicable laws differ: As compared to CIPA, Alabama and Maryland law are substantially more limited in terms of the scope of liability, enforcement mechanisms, and available remedies. Under Alabama law, (1) the interception of electronic communications is permitted where a single party consents, Ala. Code 1975 § 13A-11-30, and (2) enforcement is left to the discretion of state government, with no right of action for private plaintiffs, Ala. Code 1975 §§ 13A-11-30 to 13A-11-37. In contrast, CIPA requires the consent of all parties to a communication and allows a private right of action for injured persons. (See above). Maryland law also differs materially from CIPA. Maryland does not allow claimants to seek injunctive relief and limits civil recovery to actual damages or "liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher." Md. Code, Cts. & Jud. Proc. §10-410(a)(1). In contrast, CIPA allows claimants to seek both injunctive relief and "the greater of" $5,000 or three times the amount of any actual damages. Cal. Penal Code § 637.2(a). In short, CIPA is directly at odds with limitations that Alabama and Maryland have imposed in their respective statutes governing the interception of communications.

California has no interest in applying CIPA to the claims of non-residents: On its face, CIPA indicates that its purpose is to protect California residents, not to regulate in-state business practices that might impact non-Californians: "The Legislature by this chapter *intends to protect the right of privacy of the people of this state*." Cal. Penal Code § 630 (emphasis added). Reflecting that statement of legislative purpose, the California Supreme Court has recognized that "the principal purpose of [CIPA] is to protect the privacy of confidential communications *of California residents while they are in California*." *Kearney*, 39 Cal. 4th at 119-120 (italics in original); *see also Zephyr v. Saxon Mortg. Servs., Inc.*, 873 F. Supp. 2d 1223, 1231 (E.D. Cal. 2012) ("the purpose of [CIPA] does not appear to be to regulate out-of-state commerce or conduct, but to protect California residents").[29]

This express purpose makes clear that California has no interest in applying CIPA to

[29] *See also Kearney*, 39 Cal. 4th at 124 (noting that "one of the principal purposes underlying [CIPA]" was "protecting *individuals in California*"); *id* at 126 (noting "California's concern for the privacy of *the state's consumers*"); *id*. at 125 (noting that CIPA reflects the Legislature's effort to "increase the protection *of California consumers'* privacy") (emphases added).

claims brought by *non*-California residents, particularly where the communications at issue have no alleged link to California. This lack of a cognizable state interest is dispositive and precludes Plaintiffs from relying on California law. *Kearney*, 39 Cal. 4th at 109 (If "only one of the states has an interest in having its law applied," there is "no problem in choosing the applicable rule of law" as the law of the state having an interest.) (citation and quotation omitted)).

In contrast, Alabama and Maryland have a strong interest in applying their own laws: As a general matter, "[e]very state has an interest in having its law applied to its resident claimants." *Mazza*, 666 F.3d at 591-92 (citation and quotation omitted). Moreover, each state has a valid "interest in shielding out-of-state businesses from what the state may consider to be excessive litigation." *Id*. at 592. As the Ninth Circuit explained:

> In our federal system, states may permissibly differ on the extent to which they will tolerate a degree of lessened protection for consumers to create a more favorable business climate for the companies that the state seeks to attract to do business in the state . . . Each of our states also has an interest in being able to assure individuals and commercial entities operating within its territory that applicable limitations on liability set forth in the jurisdiction's law will be available to those individuals and businesses in the event they are faced with litigation in the future.

Id. at 592-93 (citation and quotation omitted).[30] Given these considerations, the Ninth Circuit reversed an order applying California law to the claims of non-residents because "[t]he district court did not adequately recognize that each foreign state has an interest in applying its law to transactions within its borders and that, if California law were applied to the entire class, foreign states would be impaired in their ability to calibrate liability to foster commerce." *Id*. at 593.

The same considerations preclude the CIPA Plaintiffs from applying CIPA in place of the laws of their local jurisdictions. As in *Mazza*, both Alabama and Maryland "would be impaired in their ability to calibrate liability to foster commerce" if the CIPA Plaintiffs were allowed to avoid their local laws and assert a CIPA claim. *Id*. For example, even though Alabama has

[30] Moreover, the CIPA Plaintiffs' effort to impose California law on the other 49 states would violate the Dormant Commerce Clause, particularly as applied to communications that have no connection to California. *See Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336 (1989) ("a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State.")

decided that its residents should have no private right of action to challenge an alleged interception, that legislative judgment would be entirely subverted if Alabama residents like Plaintiff Harrington could bring a CIPA claim. Similarly, the limited remedies specified under Maryland law would be meaningless if Maryland residents like Plaintiff Brad Scott could simply ignore those limitations and assert a claim under CIPA. In short, allowing Plaintiffs to bypass the restrictions of their local laws by invoking CIPA would effectively rob Alabama and Maryland of any ability to determine the appropriate scope of liability for claims brought by their residents. *Mazza* precludes this result. *See id*. at 591-94.

Indeed, the CIPA Plaintiffs' effort to impose California law on a nationwide class outside of California is in direct conflict with the claims of other Plaintiffs. While the CIPA Plaintiffs are seeking to impose CIPA to override all other state wiretapping statutes outside of California, Plaintiffs Knowles, Brinkman, and Brent Scott have chosen to rely, *not* on CIPA, but on the wiretapping statutes of their respective states of residence (Maryland, Pennsylvania, and Florida).[31] (*See* Compl. at ¶¶ 341, 361, 383.) The Court should not allow the CIPA Plaintiffs to force all non-Gmail users outside of California to rely on CIPA when three of their fellow Plaintiffs have expressly rejected the application of California law and insisted that local law must apply to their own claims and the claims of the non-Gmail users in their respective states.

V. CONCLUSION.

For all of the reasons above, Plaintiff's Complaint should be dismissed in its entirety.

Dated: June 13, 2013

COOLEY LLP
MICHAEL G. RHODES (116127)
WHITTY SOMVICHIAN (194463)
KYLE C. WONG (224021)

/s/ Whitty Somvichian
Whitty Somvichian (194463)
Attorneys for Defendant GOOGLE INC.

1319718/SF

[31] This inherent conflict is most obvious in the case of Plaintiffs Scott and Knowles. Both are Maryland residents seeking to represent a class that includes non-Gmail users in Maryland – yet Scott seeks to impose CIPA whereas Knowles has chosen to rely on Maryland law.

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXARKANA
TEXARKANA DIVISION

KEITH DUNBAR, Individually, and as Representative on Behalf of all Similarly Situated Persons,	**Civil Action N^{o} 5:10CV00194-DF**
Plaintiff,	**FIRST AMENDED**
versus	**CLASS ACTION COMPLAINT**
GOOGLE, INC.	**JURY DEMANDED**
Defendant.	

PLAINTIFF, KEITH DUNBAR, Individually and on behalf of the Class described below ("the Class"), brings this nationwide Class Action suit against Defendant Google, Inc. ("Google"), and for his First Amended Complaint,[1] and upon information and belief, alleges the following:

PARTIES

1. Plaintiff is a citizen of the State of Texas, and he resides in Bowie County, Texas, which is within the Eastern District of Texas, Texarkana, Division.

2. Google is a Delaware corporation, whose principal place of business is at 1600 Amphitheatre Parkway, Mountain View, County of Santa Clara, State of California. Google has been served through its agent for service of process: Corporation Service Company d/b/a CSC – Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701-3218.

JURISDICTION AND VENUE

3. Pursuant to 28 U.S.C. § 1331, this Court has original jurisdiction over the Plaintiff's and the Class' claims arising under the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. §§ 2510 *et seq.,* a law of the United States.

4. This Court has general and specific personal jurisdiction over the Defendant, in that Google has sufficient minimum contacts within the State of Texas and within the Eastern District of

[1] Plaintiff files his Amended Complaint pursuant to FED. R. CIV. P. Rule 15(a)(1)(B) because Defendant has yet to file a responsive pleading and 21days have not lapsed since service of the Defendant's Motion to Dismiss pursuant to Rule 12(b).

Texas, and further because certain material acts upon which this suit is based occurred within the Eastern District of Texas.

5. Venue is proper in the Eastern District of Texas pursuant to 28 U.S.C. § 1391(b) and (c) in that: (1) Google resides in the Eastern District of Texas because it is subject to personal jurisdiction within the Eastern District of Texas; (2) a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this judicial district; and (3) Google may be found in this district.

NATURE OF SUIT

6. Pursuant to Rule 23 of the *Federal Rules of Civil Procedure*, Plaintiff brings this nationwide class action lawsuit against Google for the unlawful and intentional interception of electronic communications and intentional use of the contents of electronic communications in violation of the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. Sections 2510 *et seq*. Google operates a popular email service known as "Gmail." Gmail account holders are assigned a Gmail email address through which to send and receive electronic communications. Google scans the content of all electronic communications received and sent by Gmail account holders. Utilizing a scanning or extraction device, Google intercepts all electronic communications sent to Gmail account holders. Google uses the information and content obtained from the scanning of incoming electronic communications to sell and place advertisements in Gmail account holders' browser windows that are related to the content of intercepted electronic communications.

7. Plaintiff, a non-Gmail account holder, has sent and continues to send electronic communications to Gmail account holders from non-Gmail email accounts.

8. Google intercepted(s) these electronic communications and used(s) their content for the purpose of delivering targeted advertising to the Gmail account holder recipients.

9. Neither Plaintiff nor the Gmail account holders consented(s) to the interception and use of Plaintiff's electronic communications and the contents thereof.

10. This case involves the interception of electronic communications (i.e. emails) sent from Plaintiff and other non-Gmail account holders in violation of 18 U.S.C. § 2511(1)(a).[2] It also involves the use by Google of content obtained from intercepted emails sent by the Class in violation of 18 U.S.C. § 2511(1)(d). While Google states that it presently does not disclose the content of electronic communications to third parties, Google admits that it not only intercepts and scans all emails of Gmail account holders, but Google admits that it uses the content obtained through the interception from non-consenting, non-Gmail account holders to sell and place advertisements on the Gmail account holders' browser windows. Google also intercepts and uses content from non-Gmail users' emails for purposes other than Gmail. Google intercepts and uses the information from non-Gmail users without regard to the private or proprietary nature of the information. As result of Google's actions in intercepting and using non-Gmail account holders' emails, Google obtains a monetary benefit.

11. The actions complained of herein involve the interception and use of content of Plaintiff's and Class Members' electronic communications when they are sent to a Gmail user, whether through the initialization of electronic communications to the Gmail user, a response/reply to an electronic communication from the Gmail user, or any subsequent new electronic communication transmitted by Plaintiff and Class Members to a Gmail user. This case does not involve the scanning of previously sent text from Plaintiff's and Class Members' prior emails which may be in the body of responsive communication.

STATEMENT OF FACTS

12. Google owns the world's leading internet search engine, and, as part of its marketing strategy, offers a vast array of services to internet users. Google's "free" services lure internet users, allowing Google to generate the majority of its revenues by selling online advertising aimed at the users of these "free" services. The more users or usage through Google services that can be

[2] *See* Paragraph 190 for a definition of the "Class."

demonstrated by Google to advertisers, the more revenue Google makes.

13. As part of its advertising business model, Google actively seeks out, collects, and stores vast amounts of behavioral information regarding internet users. For Google, the acquisition, storage, and ready access to information directly correspond to advertising revenues. As such, Google's advertising business model requires it to continue to acquire additional information. Personalized, detailed, and behavioral information is the most valuable to Google.

14. "Gmail" is an electronic communication service operated by Google.

15. Google requires users to register to use Gmail separate and apart from using other Google services.

16. Google assigns Gmail account holders a Gmail email address for the purposes of sending and receiving electronic communications through the electronic communication service operated by Google (i.e. Gmail). Using Google's electronic communication service, Gmail account holders can receive electronic communications from other Gmail account holders and from non-Gmail account holders.

The Contract Between Gmail Users and Google

17. In order to obtain a Gmail account and use Google's electronic communication service to send and receive electronic communications, a person must agree to the Google Terms of Service, the Google Program Policies, and the Google Privacy Policy. Each of these documents is a written contract comprising specific written clauses.

18. The Terms of Service are attached as Exhibit D. The Program Policies are attached as Exhibit G. The Privacy Policy is attached as Exhibit H.

19. To create a Gmail account, a person may view a webpage entitled, "A Google approach to Email." *See* Exhibit A.

20. The webpage entitled "A Google approach to Email" does not mention advertising.

Instead, Google touts "Lots of Space," "Less Spam," and "Mobile Access." *See* Exhibit A.

21. This webpage contains links to "Create an account," to "Terms & Privacy," and to "About Gmail." *See* Exhibit A.

22. If a person clicks on the link "About Gmail," the person is taken to a webpage entitled "Google's Approach to Email." *See* Exhibit B. This webpage gives Google's "Top 10 reasons to use Gmail." Neither advertising nor receiving targeted ads is ever mentioned.

23. At the top right of Exhibit B, "Google's Approach to Email," a big, blue rectangular button invites the user to "Get Started." Clicking that link takes a user directly to the "Create an Account" webpage attached as Exhibit C.

24. When a person clicks on the link to "Create an Account" on Exhibit A or on the inviting blue "Get Started" button on Exhibit B, the Gmail account page appears. *See* Exhibit C. After entering some personal information for the creation of the account, the person is asked to affirmatively agree to only three documents, all of which Google drafted: Google's Terms of Service, Google's Program Policy, and Google's Privacy Policy. *See* Exhibit C.

25. Google's Terms of Service is contained in a single written document entitled, "Google Terms of Service." *See* Exhibit D. When a person interested in reading the Terms of Service prints a "Printable Version" of the "Terms of Service," as allowed by Google's sign-in screen and encouraged at ¶ 2.4, a single document numbering nine (9) pages and paragraphs numbered 1.1 through 20.7 is printed. *See* Exhibit D.

26. In the "Google Terms of Service," Google expressly defines the collective word "Terms" to include only: (1) the "terms and conditions" set forth in the "Terms of Service" which Google defines as the "Universal Terms;" and (2) the "terms of any 'Legal Notices'" applicable to a specific Service, which Google defines as the "Additional Terms." *See* Exhibit D, ¶ 1.2 and 1.3. According to Google in ¶ 1.4 of the Terms of Service, only the "Universal Terms" and the "Additional Terms" form

"a legally binding agreement between [the user] and Google in relation to [the user's] use of the Services." *See* Exhibit D, ¶ 1.4.

27. At paragraph 7.1, Google refers the user to certain "data protection practices" through a hyperlink, but Google only binds the Gmail user to Google's specific Privacy Policy mentioned at ¶ 7.2. *See* Exhibit D, ¶¶ 7.1 and 7.2.

28. Paragraph 20.2 provides that "The Terms constitute the whole legal agreement between you [Gmail user] and Google and govern your use of the Services." *See* Exhibit D, ¶ 20.2. Other than the privacy policy referenced at ¶ 7.2, no other hyperlinks, webpages, documents, practices, or other terms are incorporated by reference to be included in and made a part of the "Google Terms of Service" and to create a binding agreement between Google and Gmail user.

29. Paragraph 20.7 of the Terms of Service provides that "The Terms . . . shall be governed by the laws of the State of California." *See* Exhibit D, ¶ 20.7.

30. As to the incorporated "Legal Notices," Google's Terms of Service at ¶ 1.5 specifically states, "If there is any contradiction between what the Additional Terms say and what the Universal Terms say, then the *Additional Terms shall take precedence in relation to that Service*." *See* Exhibit D, ¶ 1.5 (emphasis added). Accordingly, the Additional Terms or "Legal Notices" specific to Gmail take precedence over any conflicting provision contained in Universal Terms of the Google Terms of Service.

31. In looking at the "A Google approach to email" screen (*See* Exhibit A), there exists a link for "Terms & Privacy." Once clicked, the "Terms & Privacy" screen lists the following: Legal Notices, Privacy Policy, Program Policies, and Terms of Service. *See* Exhibit E. When the user clicks on "Legal Notices" for Gmail (also called the "Additional Terms"), a one page, two paragraph document is provided. *See* Exhibit F.

32. In the "Gmail Legal Notices," Google states its does not claim any ownership in any of

the content of any material transmitted in Gmail account. *See* Exhibit F.

33. In the "Gmail Legal Notices," Google affirmatively states to the user, "We will not use any of your content for *any purpose* except to provide you with the Service." *See* Exhibit F (emphasis added). The "Service" stated in Exhibit F is Gmail.

34. From the "Create an Account" webpage (attached as Exhibit C), the Gmail applicant is required to accept the terms of Google's Program Policy. Upon clicking the link to the "Program Policy," the reader is shown a two-page document, entitled, "Gmail Program Policies." *See* Exhibit G. No other hyperlinks, web-pages, documents, practices, or other terms are incorporated by reference to be included in and made a part of the "Gmail Program Policies." Upon printing a version of the "Gmail Program Policies" only the two page document found at Exhibit G will print.

35. In addition to other terms, the Gmail Program Policy prohibits a user from using "Gmail to violate the legal rights (such as rights of privacy and publicity) of others." *See* Exhibit G, page 1.

36. From the "A Google approach to email" webpage (attached as Exhibit A), the Gmail applicant can access the "Terms & Privacy" page at Exhibit E. Once there, the user can open Google's Privacy Policy. Upon clicking the link to the "Privacy Policy," the reader is shown a four-page document, entitled, "Privacy Policy." *See* Exhibit H. No other hyperlinks, web-pages, documents, practices, or other terms are incorporated by reference to be included in and made a part of the "Privacy Policy." Upon printing a version of the "Privacy Policy" only the two-page document found at Exhibit H will print.

37. "Google Terms of Service," "Gmail Legal Notices," "Gmail Program Policies," and Google's "Privacy Policy," (Exhibits D, F, G, H) are the only terms to which the applicant must affirmatively "accept" and agree.

Google Intercepts and Uses the Contents of Plaintiff's and Class Members' Email

38. In various webpages and through links appearing on those webpages, *none of which are*

incorporated into the Terms of Service or any binding terms upon a Gmail user, Google makes a number of admissions:

39. From a webpage entitled, "Privacy Center," Google mentions its Privacy Policy as a separate document, and then states, "The following statements explain specific privacy *practices* with respect to certain products and services." *See* Exhibit I, page 1 (emphasis added). Below the statement is a list of products and services. ***Gmail is not listed***.

40. There is no way for a user to intuit that Gmail, as a service, is related to any link referenced on the Google Privacy Center page. *See* Exhibit I.

41. In the left column of the "Privacy Center" webpage (attached as Exhibit I), there exists a link to "Advertising." When the "Advertising" link is clicked, a webpage entitled, "Advertising and Privacy" can be viewed. *See* Exhibit J.

42. Google does not incorporate by reference the information on the webpage entitled, "Advertising and Privacy," into the Google Terms of Service, the Program Policy, or the Privacy Policy.

43. In the next to the last paragraph of Exhibit J, Google states, "What information does Google use to *serve ads* on Gmail?" *See* Exhibit J, page 4 (emphasis added). Google then says:

> Google scans the text of Gmail messages in order to filter spam and detect viruses. The Gmail filtering system also scans for keywords in users' emails which are then used to match and serve ads. The whole process is automated and involves no humans matching ads to Gmail content.

See Exhibit J, page 4.

44. Google does not incorporate these words into the Terms of Service, the Program Policy, or the Privacy Policy.

45. At Exhibit J, Google only tells users it scans for "keywords" in the "users' emails."

46. However, Google also scans Plaintiff's and Class Members' emails when they are sent to Gmail users.

47. These emails are electronic communications as defined by 18 U.S.C. § 2510(12).

48. The "keywords" scanned by Google amount to content of Plaintiff's and Class Members' email.

49. Either in the scanning process, the matching process, or in some other manner, the "keywords" or content are acquired from Plaintiff's and Class Members' email by a device and matched to an advertisement. The device is automated.

50. The device is not a telephone or telegraph instrument, it is not telephone or telegraph equipment, it is not a telephone or telegraph facility, and it is not any component thereof.

51. Following the acquisition of the "keywords" or content of Plaintiff's and Class Members' email, Google uses those "keywords" or content to match advertisements.

52. On a web-page entitled "More on Gmail and privacy" (which is not accessible by links from Google's "Terms of Service," "Program Policy," "Privacy Policy," "Privacy Center," "Google's approach to email," or any page to which Google refers users regarding Gmail), Google states:

> Google scans the text of Gmail messages in order to filter spam and detect viruses, just as all major webmail services do. Google also uses this scanning technology to deliver targeted text ads and other related information. This is completely automated and involves no humans.

See Exhibit K, page 2, 3d ¶. Google further states:

> It is important to note that the ads generated by this matching process are *dynamically generated* each time a message is opened by the user—in other words, Google does not attach particular ads to individual messages or to users' accounts.

See Exhibit K, page 2, 4th ¶.

53. Google does not incorporate any of the information of Exhibit K into the Terms of Service, the Program Policy, or the Privacy Policy.

54. In Exhibit K, Google only tells user's it scans "Gmail messages."

55. Plaintiff's and Class Members' email are not "Gmail."

56. However, Google also scans Plaintiff's and Class Members non-Gmail emails when they are sent to Gmail users.

57. These emails are electronic communications pursuant to 18 U.S.C. § 2510(12).

58. The "text" of Plaintiff's and Class Members' email that is scanned by Google amounts to content of Plaintiff's and Class Members' email.

59. Either in the scanning process, the matching process, or in some other manner, the text or content is acquired from Plaintiff's and Class Members' email by a device and matched to an advertisement. The device is automated.

60. The device is not a telephone or telegraph instrument, it is not telephone or telegraph equipment, it is not a telephone or telegraph facility, or any component thereof.

61. The acquisition of content from Plaintiff's and Class Members' email occurs in the transfer of that email to the Gmail user.

62. Following the acquisition of the "text" or content of Plaintiff's and Class Members' email, Google uses the "text" or content of Plaintiff's email to generate advertisements.

63. On June 18, 2009, Nicole Wong, Deputy General Counsel for Google, testified before a House subcommittee on the privacy implication of behavioral advertising and in regard to the scanning and use of non-Gmail account holders' email and stated:

> MR. SCALISE: Do you read e-mails from people that are a Yahoo! or Google e-mail subscriber? Do you read through those e-mails to gather information in any way? . . . .
> MS. WONG: Yes. We are using that same technology that scans for viruses and also scans for spam. It is basically technology that looks for pattern text, and we use that not only for the spam blocking and viruses but also to serve ads within the Gmail user's experience so importantly like the—
>
> MR. SCALISE: So if two people are exchanging an e-mail about a sporting event and they are talking about going to the game and then maybe they are going to want to go out for a drink afterwards, could they then maybe expect to get an advertisement about which different bars are offering specials after the game?
>
> MS. WONG: They won't get an e-mail with an advertisement but only the Gmail user

> will be able to see ads that show up just like they show up on the side of our search results that are key to specific words—they are key words just as if you typed them into our browser that are calling from our repository of millions of ads to deliver an ad that is targeted to the content that you are reading.

64. Ms. Wong agreed that Google reads the email of Gmail subscribers, and Plaintiff asserts Google reads his and Class Members' non-Gmail emails when they are sent to Gmail users.

65. The "pattern text" of Plaintiff's and Class Members' email that is scanned by Google amounts to content of Plaintiff's and Class Members' email.

66. Either in the scanning process, the matching process, or in some other manner, the "pattern text" or content is acquired from Plaintiff's and Class Members' email by a device and matched to an advertisement.

67. As Ms. Wong admits, the content of Plaintiff's and Class Members' email "serve ads."

68. Ms. Wong admits that the content of Plaintiff's and Class Members' email serve as the content to which Google targets advertisements sold by Google.

69. The technology or device mentioned by Ms. Wong is not a telephone or telegraph instrument, it is not telephone or telegraph equipment, it is not a telephone or telegraph facility, and it is not any component thereof.

70. Following the acquisition of the "pattern text" or content of Plaintiff's and Class Members' email, Google uses the "pattern text" or content to sell and "serve ads."

71. Upon information and belief, and without limitation, Google utilizes an embodiment of an extraction device or devices mentioned in United States Patent Application US 2004/0059712 A1, or one similar thereto, to intercept Plaintiff's and Class Members' email and to acquire content from that email and use (*i.e.* match) that content to target advertisements displayed on the Gmail user's screen. *See* Exhibit L. The patent application was filed under the Attorney Docket No.: Google-31/CON3 (GP-064—04-US). *See* Exhibit M. Although several claims of the proposed invention were rejected on or about February 1, 2011, the Application illustrates the device(s) used by Google to intercept

electronic communications.

72. At ¶ 0087 of Exhibit L, Google's application discusses embodiments of an invention which may utilize various "devices" for the extraction or acquisition of content from in-coming email. *See* Exhibit L, ¶ 0087. In doing so, Google refers to Figure 5, block 520, entitled "Accept and/or Determine E-Mail Information," and Figure 6, block 612, entitled "Relevance Information Extraction/Generation Operations." *See* Exhibit L, ¶ 0087. In describing the "extraction operations," Google states, "an e-mail server may extract and/or generate e-mail information." *See* Exhibit L, ¶ 0087. In addition, Google states, "Indeed, e-mail information extraction and/or generation may be distributed over more than one device (e.g., e-mail application, browser, e-mail server, e-mail information server, e-mail relevant ad server, etc.)." *See* Exhibit L, ¶ 0087.

73. In addition, Google states, "Various ways of extracting and/or generating relevance information are described in U.S. Provisional Application Serial No. 60/413,536, entitled, 'METHODS AND APPARATUS FOR SERVING RELEVANT ADVERTISEMENTS', filed on Sep. 24, 2002, . . . and in U.S. patent application Ser. No. 10/314,427, entitled "METHODS AND APPARATUS FOR SERVING RELEVANT ADVERTISMENTS', filed on Dec. 6, 2002 . . . ." *See* Exhibit L, ¶ 0089.

74. The "e-mail information" of Plaintiff's and Class Members' email that is extracted by Google amounts to the content of Plaintiff's and Class Members' emails. *See* Exhibit L, ¶¶ 0046, 0051, and 0055-80.

75. The "e-mail information" or content of Plaintiff's and Class Members' email is "extracted" or acquired by Google by use of a "device" or "more than one device."

76. The device or devices are not a telephone or telegraph instrument, they are not telephone or telegraph equipment, they are not a telephone or telegraph facility, or any component thereof.

77. The interception of Plaintiff's and Class Members' email occurs during the transfer of that email to the Gmail user.

78. Following the "extraction" of "e-mail information" or content from Plaintiff's and Class Members' email, Google uses the "e-mail information" or content "for purposes of targeted ads." *See* Exhibit L, ¶ 0087.

Gmail Users Do Not Consent To Google Intercepting Email

79. Google drafted the terms and is the author of its "Terms of Service," "Gmail Legal Notices," "Program Polices," and "Privacy Policy."

80. The Google "Gmail Program Policies" (Exhibit G) do not mention the scanning, interception, or use of content of email for targeted advertising.

81. By agreeing to the terms of the "Gmail Program Policy," a user of Gmail does not consent to the interception and use of non-Gmail users' electronic communications as made the basis of this suit.

82. The Google "Privacy Policy" (Exhibit H) does not mention the scanning, interception, or use of content of email for targeted advertising.

83. By agreeing to the terms of the "Privacy Policy," a user of Gmail does not consent to the interception and use of non-Gmail users' electronic communications as made the basis of this suit.

84. Paragraph 7.1 of the "Terms of Service" refers the Gmail user to "Google's privacy policy," which can be found at a link on the web-page http://www.google.com/privacy.html. *See* Exhibit D, ¶ 7.1. Google refers the user to this policy in regard to Google's treatment of only the user's "personal information."

85. Paragraph 7.1 of the "Terms of Service" does not refer the user to any document other than the "privacy policy."

86. While the web-page identified at http://www.google.com/privacy.html is entitled the "Privacy Center," neither the "Privacy Center" nor the various hyperlinks identified on that particular page are incorporated into the "Privacy Policy" or the other terms to which the user must agree. *See*

Exhibit D.

87. The information and the hyperlinks found on the "Privacy Center" webpage do not mention the word "Gmail," and from that page a user is not given any indication that any hyperlink might contain additional information related to Gmail.

88. Paragraph 7.2 of the "Terms of Service" states that the user agrees to the use of "*your data* in accordance with Google's privacy policies." *See* Exhibit D, ¶ 7.2. The only privacy "policies" a viewer is directed to are those in the aforementioned "Privacy Policy." No other links are offered to take potential users to an actual policy other than the "Privacy Policy."

89. Paragraph 7.2 of the "Terms of Service" does not ask and does not require the user to agree to Google's use of any other person's data.

90. Paragraph 7.2 does not ask and does require the user to consent to Google's interception and use of any other person's data.

91. At ¶ 8.1 of the "Terms of Service," Google places responsibility for content to which a user may have access on the originator of the content. *See* Exhibit D, ¶ 8.1.

92. At ¶ 8.2 of the "Terms of Service," Google notifies the user that the content presented as part of the services may be owned or protected by a third party, and the user may do nothing with that content "unless you have been *specifically told* that you may do so by Google or by the owners of that Content, in a separate agreement." *See* Exhibit D, ¶ 8.2 (emphasis added).

93. At ¶ 8.3 of the "Terms of Service," Google states:

> Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service. For some Services, Google may provide tools to filter out explicit sexual content. These tools include the SafeSearch preference settings (see http://www.google.com/help/cutomoze.html#safe). In addition, there are commercially available services and software to limit access to material that you may find objectionable.

See Exhibit D, ¶ 8.3.

94. At ¶ 8.4 of the "Terms of Service," Google warns users that they may be exposed to

content that they find "offensive, indecent or objectionable and that, in this respect, you use the Services at your own risk." *See* Exhibit D, ¶ 8.4.

95. At ¶ 8.5 of the "Terms of Service," Google places sole responsibility on the user for any content created, transmitted, or displayed by user while using any of the services and for the consequences of the user's actions. *See* Exhibit D, ¶ 8.5.

96. The first sentence of ¶ 8.3 of the "Terms of Service," when viewed in the context of the entirety of Section 8 and the remaining sentences within ¶ 8.3, is limited to Google's reservation of rights to protect its services and users.

97. No wording in ¶ 8.3 advises users or seeks the consent of users for Google's interception of non-Gmail users' email.

98. No wording in ¶ 8.3 advises users or seeks the consent of users for Google's use of the content of non-Gmail users' email that have been intercepted.

99. When a user views the "Terms of Service" webpage, a link called "Terms of Service Highlights" appears in the left column. *See* Exhibit N. Google describes the "highlights" as providing users with the "basics" or a "summary" of the Terms of Service. *See* Exhibit N. In discussing the "highlights" of Google's "Terms of Service," and in particular the Section 8 highlights regarding dealing with Content, Google states:

> About your content . . . .
>
> - Content on our services usually isn't ours. *We may not monitor what we host or link to, although in some limited case we might.* Don't be surprised if you see something you don't like. You can always tell us about it or stop looking.

See Exhibit N, ¶ "About your Content" (emphasis added).

100. At Exhibit N, when Google states, "We may not monitor what we host or link to, although in some limited case we might," Google is summarizing the first sentence of ¶ 8.3 of the "Terms of Service."

101. The words "pre-screen," "review," "flag," "filter," "modify," "refuse," and "remove" are ambiguous in the context of ¶ 8.3 of the Terms of Service, Section 8 of the Terms of Service, the "Terms of Service," the "The Terms of Service Highlights," the "Gmail Legal Notices," the " Program Policies," and the "Privacy Policy" as to whether the definition of these words include the acquisition and use of content of electronic communication as made the basis of this suit.

102. Paragraph 17.1 of the "Terms of Service" advises users that "*Some* of the Services are supported by advertising revenue and may display advertisements and promotions." *See* Exhibit D, ¶ 17.1 (emphasis added). Google does not refer to Gmail as a service to which this provision is applicable.

103. Paragraph 17.1 of the "Terms of Service" further provides, "These advertisements may be targeted to the *content* information stored on the Services, queries made through the Service or other information." *See* Exhibit D, ¶ 17.1 (emphasis added). Google does not refer to Gmail as a service to which this provision is applicable.

104. At ¶ 17.1 in the "Terms of Service," Google does not advise the user how the "content" is "targeted."

105. At ¶ 17.1 in the "Terms of Service," Google does not advise the user that "content" may be from a non-Gmail user.

106. At ¶ 17.1 in the "Terms of Service," Google does not use in ¶ 17.1 the capitalized word "Content" as defined in ¶ 8.1 and used throughout the "Terms of Service."

107. Non-Gmail users do not store matters on Google's Gmail.

108. Non-Gmail users do not make queries through Gmail or other information.

109. The language of ¶ 17.1 in the "Terms of Service" is ambiguous in the context of the "Terms of Service," the "Gmail Legal Notices," "The Program Policies," and the "Privacy Policy" as to whether the definition of the words in ¶ 17.1 include the acquisition and use of content of electronic

communication as made the basis of this suit.

110. Paragraph 17.3 of the "Terms of Service" provides, "In consideration for Google granting you access to and use of the Services, you agree that Google may *place such advertising on the Services.*" *See* Exhibit D, ¶ 17.3. Paragraph 17.3 only allows Google to place advertisements on the unidentified services; it does not address or solicit consent.

111. By agreeing to the terms of the "Terms of Service," a user of Gmail does not consent to the interception and use of non-Gmail users' electronic communications as made the basis of this suit.

112. Pursuant to ¶ 1.5 of the "Terms of Service," the Additional Terms or Legal Notices for a particular Service, like Gmail, take precedence over any term within the "Terms of Service." *See* Exhibit D, ¶ 1.5.

113. The "Gmail Legal Notices" specifically states, "We will not use any of your content for any purpose except to provide you with the Service." *See* Exhibit F.

114. The electronic communication service known as Gmail is the applicable Google "Service" within the "Gmail Legal Notices."

115. Advertising is not the applicable Google "Service" within the "Gmail Legal Notices."

116. Advertising is not a Google "Service" to Gmail users.

117. Advertising is not a service within Gmail.

118. When a user subscribes to Gmail, targeted advertising is not mentioned as a service in the Gmail Terms of Service, Program Policies, and Privacy Policies.

119. On the Google web-page, "What is Gmail?" advertising is not mentioned as a service within Gmail. *See* Exhibit O.

120. On the Google web-page, "Google's approach to email, Top 10 reasons to use Gmail," advertising is not mentioned as a "reason" to use Gmail. *See* Exhibit B.

121. Paragraph 17.1 of the "Terms of Service" distinguishes "Services" from advertising

revenues which pay for the "Services." *See* Exhibit D.

122. Paragraph 17.3's specific request for the user to agree to the placement of advertisements on Services evidences that advertisements are not "Services."

123. Paragraph 17.3's specific request for the user to agree to the placement of advertisement on Services evidences that advertisements are not part of any "Service."

124. If advertisements, and in particular targeted advertisements based upon the content of Plaintiff's and Class Members' email, were a part of the Services offered by Google, the inclusion of ¶ 17.3 in the "Terms of Service" would be unnecessary.

125. Paragraphs 7.1, 7.2, 8.3, 17.1, and 17.3 are in contradiction with the "Additional Terms" entitled "Gmail Legal Notices" and are invalid to the extent they purport to allow for the interception and use of the content of Plaintiff's and Class Members' email for anything other than to provide the "user" with the Service of Gmail.

126. Paragraphs 7.1, 7.2, 8.3, 17.1, and 17.3 of the "Terms of Service" and "Gmail Legal Notices" are silent with regard to the interception and use of the content of incoming non-Gmail user's email for the purpose of delivering targeted ads.

127. Paragraphs 7.1, 7.2, 8.3, 17.1 and 17.3 of the "Terms of Service" and "Gmail Legal Notices" are ambiguous with regard to consent for the interception and use of the content of incoming non-Gmail user's email for the purpose of delivering targeted ads.

128. Previously identified Exhibit J, entitled "Advertising and Privacy," is a web-page from a link in the "Privacy Center" and listed under "Product Information." Google did not incorporate this webpage into any agreement made by the user for a Gmail account.

129. In the next to last section, entitled, "What information does Google use to serve ads on Gmail?" Google states that its filtering system scans for "keywords in *users'* emails which are then used to match and serve ads." *See* Exhibit J, page 4 (emphasis added).

130. Plaintiff's and Class Members' emails are not "users' emails."

131. The language in Exhibit J is in contradiction with the "Additional Terms" entitled "Gmail Legal Notices" and is invalid to the extent it purports to notify the user of any interception and use of the content of Plaintiff's and Class Members' email for anything other than to provide the "user" with the Service of Gmail.

132. The language of Exhibit J is ambiguous with regard to consent or notice of the interception of content of incoming non-Gmail user's email for the purpose of delivering targeted ads.

133. On the "Create an Account" screen (Exhibit C), Google states, "With Gmail, you won't see blinking banners ads. Instead, we display ads you might find useful that are relevant to the content of your messages. Learn more." Exhibit C, "Create an Account," is not part of any agreement made by the user regarding a Gmail account.

134. The phrase, "Learn more" is a hyperlink.

135. Looking at Exhibit C, Google does not identify how the "content" is obtained.

136. Looking at Exhibit C, Google only states the ads are relevant to the content of the user's messages.

137. Plaintiff's and Class Members' emails are not the "users'" messages.

138. The language in Exhibit C is in contradiction with the "Additional Terms" entitled "Gmail Legal Notices" and is invalid to the extent it purports to notify the user of any interception and use of the content of Plaintiff's and Class Members' email for anything other than to provide the "user" with the Service of Gmail.

139. The language of Exhibit C is ambiguous with regard to consent or notice of the interception of content of incoming non-Gmail user's email for the purpose of delivering targeted ads.

140. By clicking on the hyperlink, "Learn more," on Exhibit C, the applicant is taken to a webpage entitled, "Ads in Gmail and your personal data." *See* Exhibit P. Google did not incorporate

the webpage attached as Exhibit P and entitled, "Ads in Gmail and your personal data," into any agreement made by the user for a Gmail account.

141. At Exhibit P, "Ads in Gmail and your personal data," Google states, "In Gmail, ads are related to the content of *your messages*." Google further states, "Ad targeting in Gmail is fully automated, and no humans read *your email* in order to target advertisements or related information." *See* Exhibit P.

142. Google does not identify how the content is obtained.

143. At Exhibit P, Google only states the advertisements are relevant to the user's messages and the user's emails.

144. Plaintiff's and Class Members' emails are not the users' messages or the users' email.

145. The language in Exhibit P is in contradiction with the "Additional Terms" entitled "Gmail Legal Notices" and is invalid to the extent it purports to notify the user of any interception and use of the content of Plaintiff's and Class Members' email for anything other than to provide the "user" with the Service of Gmail.

146. The language of Exhibit P is ambiguous with regard to consent or notice of the interception of incoming electronic communications for the purpose of delivering targeted ads.

147. Gmail users do not consent to the interception of incoming electronic communications for the acquisition of content for targeted advertising.

148. Gmail users do not consent to the use of the content of incoming electronic communications for the purpose of targeted advertising.

149. Neither Plaintiff nor the Class Members have consented to Google intercepting and using the content of their electronic communications.

Targeted Advertising Based Upon Intercepted Content Of Email Is Not Necessary For The Rendition Of The Service Of Gmail Or For The Protection Of Google's Rights And Property And It Is Not In The Ordinary Course Of Business Of

An Electronic Communication Service

150. Pursuant to 28 U.S.C. § 2510(15), an "electronic communication service" means any service which provides to users thereof the ability to send and receive electronic communications.

151. "Gmail" is an "electronic communication service" (as defined by 28 U.S.C. § 2510(15)).

152. "Gmail" is the only "electronic communication service" (as defined by 28 U.S.C. § 2510(15)) offered by Google.

153. A Gmail account holder who sends and receives email through Gmail is a "user" pursuant to 28 U.S.C. § 2510(13).

154. A Gmail "user" (as defined by 28 U.S.C. § 2510(13)) receives Gmail through a Gmail account and through no other service of Google.

155. Emails sent and received by Gmail account holders through Gmail are "electronic communications" (as defined by 28 U.S.C. § 2510(12).

156. Although the document "More on Gmail and privacy" appears to only be locatable by an actual Google search (as opposed to certain other webpages attached as exhibit, which are located at hyperlinks in various other webpages), in Exhibit K, Google expressly states, "All major free webmail services carry advertising, and most of it is irrelevant to the people who see it." *See* Exhibit K, page 1.

157. When Google states, "All major free webmail services carry advertising, and most of it is irrelevant to the people who see it," Google admits that the "free" service or ability of a user of an electronic communication service to send and receive email can be rendered without the interception and use of content of email.

158. The acquisition and use of content from email for the purpose of displaying "relevant advertising" attached to emails sent or received through an electronic communication service is not necessary incident to the ability to send or receive email or to operate an electronic communication service.

159. "Targeted ads" in Gmail based upon the content of Plaintiff's and Class Members' email are not necessary incident to the ability for Google, if acting as an electronic communication service, to provide Gmail account holders with the ability to send and receive electronic communications.

160. In Google's case, it is the opposite. Google uses the content of Plaintiffs' and Class Members' email for target advertisements, or as Google states it, to "serve ads." As such, the service of offering free Gmail gives Google access to yet another source of behavioral information by which to sell advertisements.

161. Google has the technical capacity to offer Gmail without targeted advertisements based upon the content of email to and from Gmail users.

162. At Exhibit K, page 2, Google further states, "Google scans the text of Gmail messages in order to filter spam and detect viruses, just as all major webmail services do. Google also uses this scanning technology to deliver targeted ads and other related information." Google admits that the scanning for the protection of the service and property, as performed by the rest of the industry, is wholly separate from the delivery of targeted ads.

163. The acquisition and use of content from electronic communications for the purpose of displaying "targeted ads" attached to emails sent or received through an electronic communication service is not necessary incident to the protection of the rights or property of the provider of that service.

164. "Targeted ads" in Gmail are not necessary incident to the protection of the rights or property of Google for providing the electronic communication service known as Gmail.

165. The industry standard for webmail electronic communication services does not include the interception and use of the content of non-user's email for the purpose of delivering targeted advertising to the user of the webmail electronic communication service.

166. The ordinary course of business within the industry for webmail electronic

communication services for the ability to send and receive electronic communications does not include the interception of content of an electronic communication and the use of its content for the delivery of targeted advertisement to a user of the service.

167. Google's services that are not related to the ability to send and receive electronic communications are not electronic communication services.

168. Google's targeted advertising is not an electronic communication service as defined by 18 U.S.C. § 2510(15).

169. Google admits that it stands alone in the industry of webmail electronic communication services with its interception and use of non-user's email for the purpose of delivering targeted advertising to Gmail users.

170. Google's interception and use of content of electronic communications from Plaintiff and the Class Members for the purpose of delivering targeted advertisements to a user of Gmail is not within the ordinary course of business of an electronic communication service.

Google's Interception And Use Of The Content of Plaintiff's and Class Members' Email Is Not Limited To Targeted Advertisements To Gmail Users

171. Upon information and belief, Google's interception and use of the content of Plaintiff's and Class Members' electronic communication is not limited to the placement of targeted advertising on Gmail user's screens.

172. On September 24, 2010, Eric Schmidt, CEO of Google, stated to Charlie Rose on the PBS television network:

> CHARLIE ROSE: So how do you see the challenge from Facebook and social networking?
>
> ERIC SCHMIDT: Well, social networking is important, and Facebook is a consequential and very impressive company. And social information will be used by Google and by others, I should add, to make the quality of the results, the quality of the experience much better. The more we know about what your friends do—with your permission, and I need to say that about 500 times—we can actually use that to improve the experience that you have of getting information that you care about.
>
> CHARLIE ROSE: But at the same time, people are saying, for example, in e-

> commerce—it is more likely you want to be served by the opinions of ten friends than you are a Google Search.
>
> ERIC SCHMIDT: Well, so far the evidence is that Google search is doing very well. So if that's the future, we'll see. We can certainly make our advertising much more effective to the degree we have more information about who your friends are—and, again, with your permission, we can tie that in.

173. Google intercepts and acquires the content of Plaintiff's and Class Members' electronic communications for purposes other than Service of Gmail to users.

174. Google uses the intercepted content of Plaintiff's and Class Member's electronic communications for purposes other than the Service of Gmail to users.

175. For the purposes other than the Service of Gmail to users, Google uses the same or similar device(s) to acquire the content of Plaintiff's and Class Members' email as it does for its targeted advertisement placement in Gmail.

176. For the purposes other than the Service of Gmail, Google's interception and use of the content of Plaintiff's and Class Members' electronic communications is not an activity which is necessary incident to the rendition of Gmail or to the protection of the rights or property of Google in providing Gmail.

177. Google's interception and use of content of electronic communications from Plaintiff and Class Members for purposes beyond providing Gmail to users is not within the ordinary course of business of an electronic communication service.

178. No party to Plaintiff's and Class Members' email to Gmail users has consented to Google's interception or use of the content of Plaintiff's and Class Members' electronic communications as made the basis of this suit, to include purposes other than the Service of Gmail to users.

Plaintiff Has Sent And Continues To Send Email To Gmail Users

179. Within the Class Period, Plaintiff has sent and continues to send e-mails to Gmail account holders from non-Gmail email accounts.

180. Plaintiff's emails are electronic communications.

181. At the time Plaintiff sent the emails to Gmail account holders, Plaintiff did so from non-Gmail email accounts.

182. Google intentionally intercepted and used the content of Plaintiff's e-mails to Gmail account holders for the purpose of delivering targeted text ads and other information to the Gmail account holder and for Google's commercial gain.

183. In one specific instance and based solely on the content of Plaintiff's email, when Plaintiff's email was received by the Gmail account holder, links to competing businesses were provided for viewing by the Gmail account holder.

184. Plaintiff did not consent to Google's intentional interception and use of the content of Plaintiff's emails to Gmail account holders for the purpose of delivering targeted text ads and other information to the Gmail account holder or for any other reason.

185. Google's intentional interception and use of the content of Plaintiff's emails or the use of the information derived thereof for the purpose of delivering targeted text ads and other related information to the Gmail account holder or for other reasons provided a financial gain to Google.

186. Google did not compensate Plaintiff for the interception and use of the content of Plaintiff's email or the use of the content of Plaintiff's email for the purpose of delivering targeted text ads and other related information to the Gmail account holder or for any other reason

187. Google profited from and continues to profit from the content of Plaintiff's and Class Members' email.

188. Google's storage of Gmail user's data, including received, sent, and unsent email, to include any and all backup or other uses by Google of that data, allows Google the ability to determine the number of non-Gmail users' email sent to Gmail users for the two years prior to this suit and continuing.

189. Through Google's storage of Gmail user's email, to include any all backup or other uses by Google of that email, Google can obtain the email addresses of non-Gmail user's email sent to Gmail users for the two years prior to this suit and continuing.

CLASS ALLEGATIONS

190. Plaintiff brings this nationwide class action, pursuant to Rule 23 of the *Federal Rules of Civil Procedure*, individually and on behalf of all members of the following Class. The Class consists of:

> All persons located within the United States who sent emails from a non-Gmail account email address to a Gmail account e-mail address from within two years before the filing of this action up through and including the date of the judgment in this case (as used throughout this Complaint before and after this definition, the "Class").
>
> Excluded from the class are the following individuals and/or entities:
>
> a. Any and all federal, state, or local governments, including but not limited to their department, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions;
>
> b. Individuals or entities, if any, who timely opt out of this proceeding using the correct protocol for opting out;
>
> c. Individuals or entities, if any, who have previously settled or compromised claims(s) as identified herein for the class; and
>
> d. Any currently sitting federal judge and/or person within the third degree of consanguinity to any federal judge.

A. Numerosity

191. The Class is so numerous that joinder of all members is impracticable. Upon information and belief, the number of Gmail account holders is more than 100 million users. Correspondingly, Plaintiff alleges the numbers for the Class are in the millions.

B. Commonality

192. There are questions of law or fact common to the class. These questions include, but are not limited to, the following:

a. Whether Google intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept electronic communications in the form of Plaintiff's and Class Members' email through Gmail accounts;

b. Whether Google intentionally uses, or endeavors to use, the contents of electronic communications in the form of Plaintiff's and Class Members' email through Gmail accounts knowing or having reason to know that the information was obtained through the interception of the electronic communication in violation of 28 U.S.C. § 2511(a).

c. Whether Google acted intentionally.

d. Whether Google acquired any information concerning the substance, purport, or meaning ("content") of Plaintiff's and Class Members' email.

e. Whether Plaintiff's and Class Members' email sent to Gmail users amount to electronic communications as defined as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate commerce.

f. Whether Google uses an electronic, mechanical, or other device to acquire the content of Plaintiff's and Class Members' email, with said device meaning any device or apparatus which can be sued to intercept a wire, oral, or electronic communication and that is not any telephone or telegraph instrument, telephone or telegraph equipment, telephone or telegraph facility, or any component thereof.

g. Whether Google, through the offering of Gmail, is a provider of an electronic communication service.

h. Whether any party to the emails sent by Plaintiff and Class Members to Gmail accounts consented to the interception or use of the content of Plaintiff's and Class Members' email.

i. Whether Google's interception and use of content of Plaintiff's and Class Members' email is an activity which is a necessary incident to the rendition of providing the electronic communication service of Gmail.

j. Whether Google's interception and use of content of Plaintiff's and Class Members' email is an activity which is necessary incident to the protection of the rights or property of the Google as to Gmail.

k. Whether Google's interception and use of content of an electronic communication from a non-user of Gmail for the purpose of delivering targeted advertisements to a user of Gmail is within the ordinary course of business of a provider of an electronic communication service.

l. Whether the interception and use of content of an electronic communication from a

non-user of Gmail for purposes beyond providing Gmail to users of Gmail is within the ordinary course of business of an electronic communication service.

m. Whether the Class Members suffered actual damages as a result of Google's actions.

n. Whether Google made any profits as a result of the allegations as made the basis of this suit.

o. Whether statutory damages against Google should be assessed.

p. Whether Google should be enjoined from intercepting or using the content of Class members' emails for purposes of delivering text ads and other related information to Gmail account holders; and

q. Whether Google should be enjoined from intercepting or using the content of Class members' emails for purposes beyond the Service of Gmail.

C. Typicality

193. Plaintiff's claims are typical of the claims of the Class in that Plaintiff and the Class sent emails to Gmail account holders, Google intercepted and acquired the emails' contents for the purpose of delivering text ads and other related information to the Gmail account holders, Google intercepted and acquired the emails' contents for purposes beyond the service of Gmail, Google used or endeavored to use the contents of the Plaintiff's email and the Class emails for a the purpose delivering text ads and other related information to the Gmail account holders, Google used or endeavored to use the contents of the Plaintiff's emails and the Class emails for purposes beyond the Service of Gmail, the users of Gmail did not consent to the interception and uses made the basis of this suit, neither Plaintiff nor the Class consented to Google's interception and uses of content made the basis of this suit, Plaintiff and the Class Members have been harmed, and Google profited from the interception and use of the content of Plaintiff's Class emails.

D. Adequacy of Representation

194. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff's interests do not conflict with the interests of the Class members. Furthermore, Plaintiff has retained competent

counsel experienced in class action litigation. Plaintiff's counsel will fairly and adequately protect and represent the interests of the Class.

195. Plaintiff asserts that pursuant to Fed. R. Civ. P. 23(b)(2), Google has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

196. Plaintiff asserts that pursuant to Fed. R. Civ. P. 23(b)(3), questions of law or fact common to the Class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.

CAUSE OF ACTION
VIOLATIONS OF 18 U.S.C. §§ 2510 et seq

197. Google, as a corporation, is a "person" pursuant to 18 U.S.C. § 2510(6).

198. Throughout the entirety of the conduct upon which this suit is brought, Google's actions were/are intentional.

199. Throughout the entirety of the conduct upon which this suit is brought, Google's actions affect interstate commerce.

200. Pursuant to 18 U.S.C. § 2511(1)(a), Google intentionally intercepted, intercepts, or endeavored or endeavors to intercept the electronic communications of Plaintiff's email and Class members' emails based on the following:

- Google acquired(s) the content of Plaintiff's and Class Members' email;
- Plaintiff's and Class Members' emails are electronic communications;
- Google utilized(s) a device composing of an electronic, mechanical or other device or apparatus to intercept Plaintiff's and Class Members' electronic communications;
- Google's intercepting device is not a telephone or telegraph

instrument, it is not telephone or telegraph equipment, it is not a telephone or telegraph facility, or it is not any component thereof;

- Google does not furnish the device to Gmail users and users do not use the device for connection to the facilities;

- The device is not used by Google, if operating as an electronic communication service, in the ordinary course of its business as a provider of an electronic communication service;

- Google's interception of Plaintiff's and Class Members' electronic communications for the purpose of delivering targeted advertisements or for purposes beyond the Service of Gmail are not within the ordinary course of business of a provider of an electronic communication service

201. Pursuant to 18 U.S.C. § 2511(1)(d), Google intentionally used, uses, or endeavored or endeavors to use the contents of Plaintiff's and Class Members' electronic communications knowing or having reason to know that the information was obtained through the interception of the electronic communication in violation of 18 U.S.S. § 2511(1)(a).

202. Google's interception of and use of the contents of Plaintiff's and Class Members' electronic communications were not performed by an employee while engaged in any activity which is necessary incident to the rendition of Gmail or to the protection of the rights or property of the Google.

203. Advertising is not a service of an electronic communication service as defined by 18 U.S.C. § 2510(15).

204. Advertising is not a service of a provider of an electronic communication service as defined by 18 U.S.C. § 2510(15).

205. No party to the electronic communications sent by Plaintiff and the Class Members as made the basis of this suit consented to Google's interception or use of the contents of the electronic communications.

206. As a result of Google's violations of § 2511, pursuant to § 2520, Plaintiff and the Class are entitled to:

a. Preliminary and permanent injunctive relief to halt Google's violations;

b. Actual damages to Plaintiff and the Class and disgorgement of profits made by Google;

c. In the alternative to actual damages to Plaintiff and the Class members, for each class member the greater of $100 a day for each day of violation or $10,000 whichever is greater;

d. Punitive damages; and

e. Reasonable attorneys' fees and other litigation costs reasonably incurred.

JURY DEMANDED

Pursuant to Federal Rule of Civil Procedure 38, Plaintiff demands a jury on any issue triable of right by a jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class members, requests judgment be entered against Defendant and that the Court grant the following:

1. An order certifying the Class and appointing Plaintiff and his counsel to represent the Class;

2. Judgment against the Defendant for Plaintiff's and the Class' asserted causes of action;

3. Preliminary and permanent injunctive relief against Defendant;

4. An award of actual damages to the Plaintiff and the Class, or an award to the Plaintiff and the Class, for each, the greater of $100 a day for each day of violation or $10,000, whichever is greater; and the disgorgement of profits made by Defendant as a result of its conduct;

5. An award to the Plaintiff and Class of punitive damages against Defendant;

6. An award of reasonable attorneys' fees and other litigation costs reasonably incurred; and

7. Any and all other relief to which the Plaintiff and the Class may be entitled.

Respectfully submitted,

/s/ Sean F. Rommel
Sean F. Rommel
Tex. Bar No. 24011612
srommel@wylyrommel.com
James C. Wyly
Tex. Bar No. 22100050
jwyly@wylyrommel.com

WYLY~ROMMEL, PLLC
2311 Moores Lane
Texarkana, Texas 75503
(903) 334-8646 (Telephone)
(903) 334-8645 (Fax)

Chris Travis
Admission by *Pro Hac Vice*
Travis@gill-law.com
Drake Mann
Texas Bar No. 12929510
mann@gill-law.com

GILL ELROD RAGON OWEN & SHERMAN, P.A.
425 West Capitol Avenue, Suite 3801
Little Rock, Arkansas 72201
(501) 376-3800 (Telephone)
(501) 372-3359 (Fax)

M. Chad Trammell
Tex. Bar No. 20183750
chad@thetrammellfirm.com

THE TRAMMELL LAW FIRM, PLLC
418 North State Line Avenue
Texarkana, AR 71854
(870) 779-1860 (Telephone)
(870) 779-1861 (Fax)

ATTORNEYS FOR PLAINTIFFS

CERTIFICATE OF SERVICE

I hereby certify that on February 21, 2011, I electronically submitted the foregoing document with the clerk of the court for the U.S. District Court, Eastern District of Texas, using the electronic case files system of the court. The electronic case system sent a "Notice of Electronic Filing" to individuals who have consented in writing to accept this Notice as service of this document by electronic means. All other counsel of record not deemed to have consented to electronic service were served with a true and correct copy of the foregoing by first class mail on this date.

/s/ Sean F. Rommel
Sean F. Rommel

WYLY~ROMMEL, PLLC
Sean F. Rommel (*Pro Hac Vice*)
Email: srommel@wylyrommel.com
4004 Texas Boulevard
Texarkana, Texas 75503
Telephone: (903) 334-8646
Facsimile: (903) 334-8645

CORY WATSON CROWDER & DEGARIS, P.C.
F. Jerome Tapley (*Pro Hac Vice*)
Email: jtapley@cwcd.com
2131 Magnolia Avenue
Birmingham, Alabama 35205
Telephone: (205) 328-2200
Facsimile: (205) 324-7896

Plaintiffs' Co-Lead Counsel

CARTER WOLDEN CURTIS, LLP
Kirk J. Wolden (SBN 138902)
Email: kirk@cwclawfirm.com
1111 Exposition Boulevard, Suite 602
Sacramento, California 95815
Telephone: (916) 567-1111
Facsimile: (916) 567-1112

Plaintiffs' Liaison Counsel

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE GOOGLE INC. GMAIL LITIGATION	Master Docket No.: 13-MD-02430-LHK
THIS DOCUMENT RELATES TO: ALL ACTIONS	**PLAINTIFFS' OPPOSITION TO GOOGLE INC.'S MOTION TO DISMISS** Date: September 5, 2013 Time: 1:30 p.m. Judge: Hon. Lucy H. Koh Place: Courtroom 8—4th Floor

///

///

///

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **PAGE**

STATUTES

I. STATEMENT OF ISSUES

1. Google's undisclosed interception, extraction, acquisition, and use of the substance, purport, and meaning of the content of the Plaintiffs' email messages violates ECPA, and its Florida, Maryland, and Pennsylvania state law analogues because:

- As to the facts of this case, ECPA's ordinary course of business exception applies only to actions necessary for Google to offer "to users thereof the ability to send or receive wire or electronic communications" [1];
- No email user consents to Google's undisclosed message-content extraction and acquisition because: (1) Google's conduct is secret; (2) Google's express terms forbid the conduct; (3) Google violates its own agreements with users through its conduct; and, (4) Google's minor users have no capacity to consent; (5) Google's actions are beyond that necessary for it to offer "to users thereof the ability to send or receive wire or electronic communications";[2] and,
- Google's affirmative defense of consent is not amenable to resolution on a pleadings motion.

2. Google's reading, learning, and recording of the meaning and content of private communications violates CIPA because:

- CIPA protects emails which are electronic "communications" or "messages" from Google's unlawful interceptions;
- The *Scott I* Plaintiffs specifically allege a California connection pursuant to CIPA that Google ignored; and
- All CIPA Plaintiffs have standing to pursue their claims because they have been injured by Google's violation of their statutory privacy rights.

II. INTRODUCTION

Separate from the normal web-mail processing for SPAM, viruses, spellchecking, routing and delivery, storage, and/or the placement of an email message in a user's inbox, Google actually diverts email messages to separate devices to extract the meaning from the message. These separate devices do not deliver the message, nor do they simply spell-check, index, or highlight words. Google designed these devices to capture the authors' actual *thoughts* ("thought data") for Google's secret use. Any other definition of "automated processing" or "automated scanning" used in the context of this Motion is irrelevant and ignores the Complaint's recitation of the actual practices at issue. (CC, ¶¶ 22-96.)

///

[1] *See* 18 U.S.C. 2510(5)(a)(ii), 2510(14), and 2510(15).
[2] *Id.*

Google creates and uses this "thought data" and attaches it to the messages so Google can better exploit the communication's "meaning" for commercial gain. Google collects and stores the "thought data" separately from the email message and uses the "thought data" to: (1) spy on its users (and others); and, (2) amass vast amounts of "thought data" on millions of people (secret user profiles). Google's attempt to describe its "thought data" mining generically as "automated processing" or "automated scanning" improperly rewrites Plaintiffs' allegations.

Google does not disclose its "thought data" mining to anyone. Google's undisclosed processes run contrary to its expressed agreements. Google even intercepts and appropriates the content of minors' emails despite the minors' legal incapacity to consent to such interception and use. Thus, these undisclosed practices are not within the ordinary course of business and cannot form the basis of informed consent. Despite Google's proclamation, Google cannot do "as it wishe[s]" with the private communications of millions of unsuspecting users and third parties in violation of the privacy protections afforded by the statutes at issue here. Accordingly, Google's motion should be denied.

III. STATEMENT OF FACTS

Plaintiffs provide the following facts supported by the ***actual*** allegations in the Complaint.

A. Gmail—The Secret Data Mining Machine

Google uses Gmail as its own secret data mining machine which intercepts, warehouses, and uses, without consent, the private thoughts and ideas of millions of unsuspecting Americans who transmit email messages through Gmail. (CC, ¶¶ 19-98.) The Complaint does not seek to prohibit reliable delivery of email or processes designed to "***scan*** email content to filter out spam… [or] detect computer viruses[.]" (Doc. 44, "MTD", 3:22-23.) This case is about Google's undisclosed practices which go beyond normal web-mail "automated ***scanning***" by using ***additional devices*** that intercept messages while in transit to the recipient and ***extract***, ***acquire***, and ***use*** email message content to determine the sender's actual thoughts and ideas. (CC, ¶¶ 22-39, 40-98.) Google stores and uses this extracted information to monitor, spy, and build secret user profiles on millions of people. (CC, ¶¶ 4, 94-98.) Google also uses this

information for its own financial benefit to avoid traffic acquisition costs and increase profits. (CC, ¶¶ 96, 282, 338, 358, 380.) Google's undisclosed practices of intercepting, reading, extracting, acquiring, and using private email content are unique among email service providers, and its nefarious data mining practices stand alone. (CC, ¶¶ 257, 259f-g, 262-63, 331-32, 352-53, 374-75.)

B. No Person Consents to Google's Secret Data-Mining Practices.

No one consents to Google's undisclosed data mining where Google (1) intercepts email messages in transit to acquire meaning, collect content, create metadata, and collect that information for subsequent use; and, (2) reads email messages to obtain the "actual ideas in a person's mind," or "thought data"; all *regardless* of whether a person receives advertising.

Plaintiffs' factual allegations, conveniently ignored by Google, challenge in detail Google's attempt to manufacture consent based on its inadequate terms and disclosures. (CC, ¶¶ 102-213.) Despite Google's attempt to substitute its own version of the facts, a jury—not Google—must decide whether persons consent to Google's undisclosed content extraction, acquisition, and use practices.

C. Google Apps—The Fraud Upon End-Users

As a subset of Gmail, Google offers Google Apps, a paid service used by businesses, educational organizations, and ISPs. (CC, ¶¶ 20, 100-01.) The express terms of the agreements between the users and Google forbid Google from serving advertisements. (CC, ¶¶ 100-01, 137-84.) Further, the agreement limits Google's access to user emails. (CC, ¶¶ 137-145.) Although Google Apps users do not receive advertisements, Google still secretly intercepts and spies on every message and reads, extracts, acquires, collects and uses the content to create, collect, use, and store "thought data." (CC, ¶¶ 100-01.) This fact demonstrates that Google's data-mining practices are not for the benefit of the user, but for Google. And, Google does not disclose this unlawful practice to users in any of its terms or disclosures. (CC, ¶¶ 102-21.)

///

///

///

IV. ARGUMENT

Accepting "all factual allegations in the complaint as true,"[3] Plaintiffs have alleged a *prima facie* case for violations of ECPA—and ECPA's Florida, Maryland, and Pennsylvania state law analogues—because Plaintiffs have pleaded facts establishing "that [Google] (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device." *Blumofe v. Pharmatrak, Inc. (In Re Pharmatrak, Inc. Privacy Litig.)*, 329 F.3d 9, 18 (1st Cir. 2003). *Compare* 18 U.S.C. § 2511(1)(a)[4] *with* (CC, ¶¶ 19-101, 214, 215-86, 322-84.) Plaintiffs also pleaded that Google's unlawful conduct includes: (1) an intentional act; (2) an interception; and, (3) a use of content. *Compare* 18 U.S.C. § 2511(1)(d) *with* (CC, ¶¶ 19-101, 214, 260.)

Plaintiffs have also pleaded two of "three distinct and mutually independent" violations of Cal. Penal Code § 631: "willfully attempting to learn the contents or meaning of a communication in transit over a wire, and attempting to use or communicate information obtained as a result of engaging in [] the previous [] activities." *Tavernetti v. Superior Court of San Diego County*, 22 Cal. 3d 187, 192-93 (Cal. 1978). *Compare* Cal. Penal Code § 631 *with* (CC, ¶¶ 19-101, 214, 287-97, 298-309).

Finally, Plaintiffs have pleaded facts establishing violations of Cal. Penal Code § 632: that Google "intentionally and without consent of all parties to a confidential communication . . . records the confidential communication . . . by means of a telegraph, telephone, or other device, except a radio . . . ." Cal. Penal Code § 632(a). *Compare* § 632 *with* (CC, ¶¶ 19-101, 214, 287-97, 310-20). Google cannot escape Plaintiffs' well-pleaded Complaint.

A. Google's Extraordinary Practice of Email Content Extraction, Acquisition, and Use is NOT an "Ordinary Course of Business."

In *Dunbar*, Google already lost its "exception" argument on its previous motion to dismiss. *Dunbar, et al. v. Google, Inc.*, 5:10-cv-194, Doc. 61, p. 7-8 (E.D. Tex. May 23, 2011).

///

[3] *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007).

[4] Citations to specific provisions of ECPA should be construed as citations to the respective portions of each of the Florida, Maryland, and Pennsylvania analogue state statutes.

1. No Exception Applies to Google's Extraordinary Practice of Email Interception, Content Extraction, Acquisition and Use.

No generic "automated processing," "automated scanning," or general electronic communication service provider ("ECSP") exception exists within ECPA. Congress carved out one ECSP exception applicable here. Section 2510(5)(a)(ii) exempts from liability "devices" used by wire and ECSPs "in the ordinary course of its business." This exception, however, does not apply to Google's devices which extract, acquire, and use email content and which are not incident to the safe delivery of email. Yet, Google seeks a construction that ***any*** "processing" performed by an ECSP is excluded from liability under ECPA as long as the particular provider deems the act to be within its own ***subjective*** "ordinary course of its business." In effect, Google advocates for an ECSP exemption that would swallow the rule, destroy the very protections afforded by ECPA, and allow every telecommunication and email provider to self-define the limits of its own power—which Google contends is limitless.[5]

The ***only*** "ordinary course of business" language applicable here derives from 18 U.S.C. § 2510(5)(a)(ii) and from within the definition of the word "device." Critical to the analysis of this exception is an understanding that an unlawful interception requires a "device." The operative language of 18 U.S.C. § 2510(5)(a)(ii) states:

> 'electronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire . . . or electronic communication other than—(a) any telephone or telegraph instrument, equipment, or any component thereof . . . (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business. . . .

The statute limits the ordinary course of business exception to "electronic communication service" providers and only where the provider acts in the "ordinary course of its business." Plaintiffs assert the "ordinary course of business" exception applies only to the

[5] Google's efforts to interject components of the Stored Communications Act have no application in this case because: (1) this case does not involve an ECSP accessing information from storage as contemplated by § 2701, (2) the entirety of Plaintiffs' Complaint challenges whether Google was "authorized" to act; and, (3) such a reading of § 2701 would render meaningless § 2510(5)(a)(ii) of the Wiretap Act because, according to Google, all acts by an ECSP within its facilities are covered by § 2701. Finally, Google's expansive version of §§ 2701-03 renders meaningless every analysis by every court on the differences between "storage" and "transmission"/"in transit" when looking at the differences between the application of § 2511 and § 2701. No court has ever sanctioned such an application of §§ 2701-03 to allegations of "interceptions."

provider's "basic service"[6] necessary to "properly route, terminate and otherwise manage"[7] email messages. Google claims that the "ordinary course of business" exception encompasses ***every subjective business practice*** of a provider of a wire or electronic communication service. Unless every subjective business practice is subject to a blanket exception, factual determinations are required to decide whether Google's interception, content extraction, acquisition, and use are beyond the exception.

While ECPA does not define "ordinary course of its business," the statutory language reveals the limitations to the exception. First, Congress did not *exempt* providers of wire or electronic communication services from ECPA's application.[8] As the Ninth Circuit opined, "the authority to intercept and disclose wire communications is not unlimited[.]" *United States v. Cornfield*, 563 F.2d 967, 970 (9th Cir. 1977) (limiting actions to those necessary for the rendition of service and protection of rights and property). Section § 2510(5)(a)(ii) expresses Congress's intent to limit the exceptions for only *particularized* conduct.

Second, the § 2510(5)(a)(ii) limitation is only applicable to "providers" of wire or "electronic communication services." Congress defined an "electronic communication system" to mean those facilities used for the "*transmission* of wire or electronic communications." 18 U.S.C. § 2510(14)(emphasis added). Section 2510(15) defines an "electronic communication service" as "any service which provides to users thereof the ***ability to send or receive wire or electronic communications.***" 18 U.S.C. § 2510(15)(emphasis added). Businesses or *services* beyond the "ability to send or receive wire or electronic communications" are not by definition "electronic communication services." Facilities or systems unrelated to "transmission" are not electronic communication systems. The definitions enacted by Congress establish that the limited business upon which the exception was created was for the "ability to send or receive wire or electronic communications."

///

---

[6] *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 505 (2d Cir. 2005).

[7] (MTD, 7:2-6, quoting the legislative history of ECPA, S. Rep. No. 99-541.)

[8] Plaintiff intentionally left in the word "wire" communications because Google's interpretation would allow every telephone communication provider to unlawfully record and commercially use the communications of every telephone call in the United States.

The congressional history cited by Google actually supports Plaintiffs' contention that § 2510(5)(a)(ii) is limited to an ECSP's ability "to monitor a stream of transmission ***in order to properly route, terminate, and otherwise manage the individual messages they contain.***" (MTD, 7:2-6) (emphasis added.) Nothing in ECPA or the legislative history allows providers like Google to bootstrap other acts beyond those necessary for the routing, termination, or management of the message. The Second Circuit's opinion in *Hall* also supports Plaintiffs' construction of the limited application of § 2510(5)(a)(ii). The *Hall* court applied the exception for the provider "because ***their basic services*** involve the 'acquisition of contents' of electronic communications." *Hall*, 396 F.3d at 505 (emphasis added). The *Hall* court didn't exempt "any services," it excepted "basic services."

Courts have also limited the "ordinary course of its business" language within § 2510(5)(a)(i) and the law enforcement component of § 2510(5)(a)(ii) to thwart attempts to expand the scope of the exception. As the Eleventh Circuit stated, "It is not enough for [defendant] to claim that its general policy is justifiable as part of the ordinary course of business. We have no doubt that it is." *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983). "[T]he phrase 'in the ordinary course of business' cannot be expanded to mean anything that interests a company. Such a broad reading 'flouts the words of the statute and establishes an exemption that is without basis in the legislative history' of Title III." *Id.,* 704 F.2d at 582 (quoting *Campiti v. Walonis*, 611 F.2d 387, 392 (1st Cir. 1979). Likewise, Chief Judge Posner denounced an ***unlimited*** "ordinary course of [his duties]" exception for law enforcement personnel:

> Investigation is within the ordinary course of law enforcement, so if "ordinary" were read literally warrants would rarely if ever be required for electronic eavesdropping, which was surely not Congress's intent. Since the purpose of the statute was primarily to regulate the use of wiretapping and other electronic surveillance for investigatory purposes, "ordinary" should not be read so broadly; it is more reasonably interpreted to refer to routine noninvestigative recording of telephone conversations. (This interpretation may have much the same practical effect as the interpretation mentioned earlier in which "ordinary course" refers to recording calls on one's own line; for ordinarily when police record calls as part of an investigation they are recording calls on someone else's line.) Such recording will rarely be very invasive of privacy, and for a reason that does after all bring the ordinary-course exclusion rather close to the consent exclusion: what is ordinary is apt to be known; it imports implicit notice.

Amati, et. al v. City of Woodstock, 176 F.3d 952, 955 (7th Cir. 1999)(emphasis added). The Sixth Circuit also requires *knowledge* of the action to make it "ordinary." *See Adams v. City of Battle Creek,* 250 F.3d 980, 984 (6th Cir. 2001). Congressional intent, statutory purpose, and case law narrowly limit the "ordinary course of business" exception to those services and processes which enable providers the ability to offer "to users thereof the ability to send or receive wire or electronic communications."

Section 2510(5)(a)(ii)'s exception is limited to acts necessary to deliver messages is confirmed by its companion exception, 18 U.S.C. § 2511(2)(a)(i), which protects *employees*[9] of providers while they are engaged in acts "necessary incident to the rendition of his service" or to "the protection of the rights or property of the provider." Through § 2511(2)(a)(i), Congress sought to insulate employees engaged in the service of the transmission of a communication. It would be inconsistent to protect these same employees for such a limited purpose but expose only the employees to liability for a company's actions beyond the acts "necessary incident to the rendition of service.

Thus, all statutory language and relevant authority support that § 2510(5)(a)(ii) applies only to those actions necessary to transmit or deliver wire of electronic communications.[10] Google's interpretation strays from Congressional intent and would allow any provider to bootstrap any subjective business interest as "its ordinary course of business" with no objective way to rebut the assertion. Plaintiffs allege that the devices used by Google to perform its unlawful acts are "separate and distinct pieces of Gmail infrastructure" and are not used for the ability to send or receive electronic communications. (CC, ¶¶ 22-90, 214, 259e-f, and 261-265.) Such facts can be applied objectively to the statute to deny Google's Motion.

2. No Court Has Ever Ruled That Google's Practices of Content Interception, Extraction, Acquisition and Use are Lawful.

While Google hypnotically repeats the expression "automated processing" to make its undisclosed practices seem innocuous, this case presents ECPA issues of first impression. No

[9] Google has failed to explain how its "automated processing," which it claims involves no "humans," would ever fall within the protection of § 2511(2)(a)(i). (*See* CC, ¶¶ 261, 330, 351, and 372.)

[10] *See* 18 U.S.C. 2510(5)(a)(ii), 2510(14), and 2510(15); *Hall,* 396 F.3d at 505; *Amati,* 176 F.3d at 955; and *Adams,* 250 F.3d at 984.

court has ever been confronted with a web-mail service that: (1) intercepts and acquires meaning and "thought data" from every email message in transit, collects content from email messages, creates metadata, and attaches that information to the email message for subsequent use; (2) intercepts and reads email messages to obtain the "actual ideas in a person's mind" ("thought data"); (3) creates surreptitious and catalogued profiles on people—all in violation of its own user agreements. Plaintiffs pleaded that the devices at issue are not used by Google for the ability to send or receive communications and are not used by others in the industry. Under these facts, Google's reliance on *Kirch* and *In re Google Privacy Policy* are not helpful. Twice, the court in *Kirch* commented, "We need not decide where to draw the line between *access* to data and *acquisition* of data." *Kirch v. Embarq Management Co.,* 702 F.3d 1245, 1249, and 1251 n.3 (10th Cir. 2012)(highlighting repeatedly that defendant never acquired any information). *Kirch* is inapposite because Plaintiffs allege Google *does acquire* data from email.

Likewise, Google erroneously asserts that Judge Grewal held ECPA does not apply to its ECSP facilities. ECPA does apply to the internal systems of an ECSP, or else there would be no need for the exceptions to the statute enumerated at § 2510(5)(a)(ii) or 2511(2)(a)(i)—Congress could have simply declared the "electronic communications systems" or "facilities" of "electronic communication services" to be exempt. Even so, unlike the plaintiffs in *In re Google Privacy Policy*, Plaintiffs here have alleged that the devices at issue are "outside" those "systems" necessary for the transmission of email in a service providers' ordinary course of business. *See In re Google Privacy Policy*, 2012 WL 6738343 at *5-6 (N.D. Cal. 2012). Unlike the insufficient allegations in *In re Google Privacy Policy*, here Plaintiffs allege that Google diverts email messages to the accused devices, which are separate and distinct pieces of Gmail infrastructure, to acquire and use the message content.

3. Plaintiffs Allege Conduct Beyond The Ordinary Course of Business

The Complaint details factual reasons why Google does not operate in the ordinary course of business: (1) Google's actions violate its agreements with its users[11] and contracting

[11] *See* CC, ¶¶ 119-20, 132, 134, 142, 145, 149-50, 153, 156-57, 173-74, 177, 179-81, 191, 193, and 195.

parties like Cable One and EDU customers;[12] and, (2) all of Google's disclosures, are materially inadequate and fraudulent.[13] Unless Google contends that breaches of contracts and the dissemination of false and misleading information are within its ordinary course of business, Google cannot overcome Plaintiffs' pleading. Further, Google's actions are undisclosed. *See Adams*, 250 F.3d at 984 (ordinary course of business requires "notice"). Accordingly, Google's actions are not "ordinary."

Finally, *no other* ESCP acts the way Google does—using extraneous devices beyond the reliable delivery of email to acquire and use personal communication content.[14] Google falsely asserts that Yahoo! performs the same acts Plaintiffs allege against Google. (MTD, 3-4, n.1.) Google omitted that it was a ***co-defendant*** with Yahoo! in the matter of *Julie Sheppard v. Google, Inc., et al.*[15] where Yahoo! filed a ***sworn declaration*** stating:

> I am familiar with the Complaint filed in this action, and aware that the plaintiffs contend that, prior to delivery, Yahoo! intercepts and reads personal emails sent from non-Yahoo! Mail users to Yahoo! Mail users. However, with the exception for scanning for viruses, malware and spam, Yahoo! ***does not engage in that practice.***

(Declaration of Amir Doron, Doc. 51-2, Exhibit A to Tapley Dec.).[16] It is not a "standard" in the industry if no one else does it, and Google's data mining of personal email messages stands alone.

4. Google's Interpretation Would Destroy ECPA's Privacy Protections

Plaintiffs do not seek to criminalize SPAM control, virus protection, or routing of email messages. Google can even lawfully perform any of the undisclosed practices Plaintiffs uncovered in discovery—as long as Google *properly* obtains informed consent before doing so. But, Google does not.

///

[12] *See* CC, ¶¶ 139, 142, 156-57, 163, 166, 169, and 179-81.
[13] *See* CC, ¶¶ 201-08, and 211-12.
[14] *See* CC, ¶¶ 257, 262-63, 331-32, 352-53, and 374-75.
[15] *See Julie Sheppard v. Google, Inc., and Yahoo!, Inc.,* 4:12-cv-4022, In the United States District Court for the Western District of Arkansas, Texarkana Division.
[16] Despite Google's implications in Footnote 1, Yahoo! was dismissed on an unopposed motion in both *Penkava* and *Sheppard* based upon a sworn statement by Yahoo! that it doesn't do what Google claims.

Allowing any telephone company or web-mail service provider to simply declare any course of business or "automated process" as a legitimate § 2510(5)(a)(ii) exception would destroy ECPA's privacy protections. Every ECSP "device" would be exempted under Google's interpretation. In effect, Google and *every single* ECSP or telephone company using "automated processing" could begin selling actual private conversations and emails to any third-party because there would be no device, no interception, and no barrier to disclosure.

Congress never envisioned and never enacted the breadth of the exception for which Google advocates. Section 2510(5)(a)(ii)'s "ordinary course of its business" must be limited to those actions necessary to provide to users "the ability to send or receive wire or electronic communications." Nothing more. If an ISP or ECSP offers additional services to set itself apart from the industry, ECPA requires honest disclosure and adequate consent.[17]

5. Plaintiff Brinkman Properly Alleges An "Interception" Under Pennsylvania Law

Google seeks dismissal of the Pennsylvania Class's received claims. (MTD 13:7-19.) Google does not challenge Brinkman's ***sent*** claims, but Brinkman has clearly pleaded that she sent emails that were intercepted by Google. (CC, ¶¶ 364, 367, 370, and 391.) Google challenges Brinkman's ***received*** claims (CC, ¶¶ 365-67, and 391), relying upon both *Klump v. Nazareth Area Sch. Dist.*, 425 F. Supp. 2d. 622, 633 (E.D. Pa. 2006), and *Kline v. Security Guards, Inc.*, 386 F.3d 246, 257 (3d Cir. 2004). (MTD, 13.) In *Kline*, the Third Circuit adopted a test that requires plaintiff to have "engaged in . . . [a] communication." *Kline*, 386 F.3d at 257. *Klump* incorrectly applied *Kline* by defining "engaged in" to exclude the intended recipient of a communication as a party who is "engaged in . . . [a] communication," despite the ordinary definition of that term or the fact that a "communication" necessarily requires a sender and at least one recipient. This Court should rely upon the Third Circuit's analysis in *Kline* **without** *Klump*'s unsound definition of "engaged in."

///

///

[17] Requiring consent for extraneous acts beyond delivery of email has far fewer consequences than a subjective, boundless exception, which would wreak havoc on privacy rights.

B. No Person Consents To Google's Conduct

In *Dunbar*, Google already lost its consent argument on its previous motion to dismiss. *Dunbar, et al. v. Google, Inc.*, 5:10-cv-194, Doc. 61, p. 7 (E.D. Tex. May 23, 2011).

Google's consent arguments fail for a number of reasons. First, as "the party seeking the benefit of the exception," Google has the burden of proving consent. *In re Pharmatrack, Inc.*, 329 F.3d at 19. However, "[C]onsent is an affirmative defense to an ECPA claim that need not be anticipated by Plaintiffs in the pleadings." *Valentine v. Wideopen West Fin., LLC*, 288 F.R.D. 407, 413 (N.D. Ill. 2012).[18]

Second, consent may be express or implied, but "[i]mplied consent is not, however, constructive consent. Rather, implied consent is 'consent in fact' which is inferred from surrounding circumstances indicating that the party *knowingly agreed* to the surveillance." *Williams v. Poulos*, 11 F.3d 271, 281 (1st Cir. 1993)(emphasis in original)(quoting *Griggs-Ryan v. Smith,* 904 F.2d 112, 116-17 (1st Cir. 1990)). *See also Berry v. Funk*, 146 F.3d 1003, 1011 (D.C. Cir. 1998)("Without actual notice, consent can only be implied when 'the surrounding circumstances [] convincingly show that the party knew about and consented to the interception.'")(quoting *United States v. Lanoue*, 71 F.3d 966, 981 (1st Cir. 1995)). Further, Consent "should not casually be inferred," *In re Pharmatrack, Inc.*, 329 F.3d at 20, nor "cavalierly implied," *Watkins*, 704 F.2d at 581. The Complaint details the secrecy of Google's nonconsensual data mining practices and explains how that secrecy prevents any inference or implied understanding of Google's conduct. (*See* CC, ¶¶ 22-91, 102-213.)

Finally and most importantly, consent may be limited: "A party may consent to the interception of only part of a communication or to the interception of only a subset of its communications." *Pharmatrack, Inc.,* 329 F.3d at 19. As such, a court "must inquire into the *dimensions of the consent* and then ascertain whether the interception exceeded those boundaries." *Id*., *quoting Gilday v. DuBois*, 124 F.3d 277, 297 (1st Cir. 1997). *See also Griggs-Ryan,* 904 F.2d at 119. As the Eleventh Circuit explained in *Watkins*: "consent within the meaning of section 2511(2)(d) is not necessarily an all or nothing proposition; it can be

[18] Consent is—with the exception of the *Dunbar* claims where Google has answered twice already—only an expected affirmative defense because Google has not yet answered.

limited. ***It is the task of the trier of fact to determine the scope of the consent*** and to decide whether and to what extent the interception exceeded that consent." *Watkins*, 704 F.2d at 582 (emphasis added). The undertaking of such an analysis in the face of the detailed Complaint would alone be sufficient to deny Google's motion.

Accepting the Plaintiffs' allegations as true, Google must demonstrate what it cannot—that the Complaint reveals facts that Google ***actually*** disclosed its practice of intercepting, extracting, acquiring, and using email content, while in transit, to obtain the sender's actual thoughts and ideas, and which it uses for purposes like creating secret user profiles. To avoid this standard, Google asks this Court to apply an imaginary standard: that consent for ***any*** purpose (automated processing for routing or viruses) = consent for ***every*** purpose (extraction, acquisition, and use of email content). Under Google's standard, if users consent to "automated processing" for virus protection, users consent to "automated processing" for all purposes, regardless of whether Google discloses those processes and purposes. No such standard for consent exists because consent "***must be actual*** " and for "***such*** interception." *In re Pharmatrack, Inc.*, 329 F.3d at 19 (emphasis added); *see also* 18 U.S.C. § 2511(2)(d)(emphasis added).

Because consent is an affirmative defense to an ECPA claim, the Court can dismiss a claim pursuant to an affirmative defense "only if the defense is 'clearly indicated' and 'appears on the face of the pleading.'" *Valentine, LLC*, 288 F.R.D. at 413; *see also Harris v. Amgen, Inc.*, 2013 U.S. App. LEXIS 11223 at *47 (9th Cir. 2013).[19] Plaintiffs' Complaint details Google's unlawful practices that include multiple devices (separate from Google's "automated processes" like spam filtration and virus detection), the routing of messages to these devices, interceptions by these devices, and the acquisition of the content and meaning of the messages by these devices. (*See* CC, ¶¶ 22-98, and 214.) Plaintiffs' Complaint further explains how these secret, separate devices that perform separate interceptions and exploit the acquired information are (1) undisclosed; and, (2) contradict Google's own written word. (*See* CC, ¶¶

[19] *See also Harris*, at *47, noting that *Jones v. Bock*, 549 U.S. 199, 211-12 (2007), "[held] that a plaintiff need not plead the absence of an affirmative defense, even a defense like exhaustion of remedies, which is 'mandatory.'"

102-213.) By ignoring these detailed factual allegations, Google fails its burden. Nevertheless, Plaintiffs are required to address Google's generalized consent arguments below.

1. Google Fails To Address Plaintiffs' Specific Allegations Regarding Its Terms and Disclosures

Google sidesteps Plaintiffs' allegations addressing user agreements with Google: the TOS, Privacy Policy, and the Gmail Legal Notice. The Complaint details the failure of Google's "Terms of Service" to honestly inform users of Google's interceptions and use of their data. (*See* CC, ¶¶ 102-136.) Google cannot, as a matter of law, overcome Plaintiffs' specific allegations regarding certain sections of the various terms and policies or its violations of agreements with third parties like Cable One and the University of Hawaii. *See* CC, ¶¶ 107-114 (detailing § 17.1's inapplicability to email and Google's removal of § 17.1 *after* March of 2012).[20] Google not only ignores Plaintiffs' rebuttal of § 8.3's application[21] (*see* CC, ¶¶ 104-106), but it also ignores the well accepted principle of law, "knowledge of the ***capability of monitoring*** alone" is not sufficient for consent. *Watkins,* 704 F.2d at 581[22]

The Complaint reveals Google's TOS and Privacy Policy actually prohibit the very conduct at issue. Citing to the "use" language of its Privacy Policy (MTD, 15:11-18), Google fails to address ¶¶ 187-90 of the Complaint detailing how Google's policies affirmatively *limit the collection* of users' information—contrary to Google's actual practices. Google cannot "use" what Google cannot "collect." Finally, none of the cases cited by Google are analogous to the detailed allegations in this case explaining how Google's TOS and Privacy Policy prohibit the undisclosed data mining practices at issue here.

///

///

///

///

[20] Section 17.1 is further inapplicable to Google Apps and Google EDU users because by contract they cannot be served advertisements. *See* CC, ¶¶ 158, 169-70.

[21] Section § 8.3 of the TOS does not state that Google ***will*** monitor. Section 8.3 actually states, "Google reserves the right (but shall have no obligation) to" perform the various acts. Plaintiffs specifically averred § 8.3 was merely a "reservation of rights." *See* CC, ¶ 105.

[22] *See also Deal v. Spears*, 980 F.2d 1153, 1157 (8th Cir. 1992).

2. The Minor Plaintiffs Cannot Consent To Google's Actions

i. Pursuant to Section 6701 of the California Family Code, minors have no capacity to consent to Google's unlawful actions.

Under California law, a minor has no capacity to "give a delegation of power" or "make a contract relating to any personal property ***not in the immediate possession or control*** of the minor." Cal. Fam. Code § 6701 (emphasis added). Section 6701 codifies "the law to protect a minor against himself and his indiscretions and immaturity as well as against the machinations of other people and to discourage adults from contracting with an infant."[23] *Berg v. Traylor*, 148 Cal. App. 4th 809, 818 (Cal. App. Ct. 2007). The statute's express language, prohibiting a minor's "delegation of power" and requiring that a minor have "immediate possession or control" of the property at issue, confirms that under California law "a minor cannot contract with respect to a future interest." *Sisco v. Cosgrove,* 51 Cal. App. 4th 1302, 1307 (Cal. App. Ct. 1996).

Plaintiff J.K.'s data contained in his Gmail messages are his personal property. Under California law, *all* property is either "real" or "personal." Cal. Civ. Code § 657. Because Gmail message data is not real property, it is, by definition, "personal property."[24] Further, the Ninth Circuit has declared such intangible property as personal property. *See Kremen v. Cohen,* 337 F.3d 1024, 1034 (9th Cir. 2002).[25] J.K.'s data within Gmail is "personal property" within the language of § 663 and modern law regarding the electronic medium at issue.

Furthermore, at the moment of Google's unlawful acts, Plaintiff J.K.'s personal property—the data contained in his Gmail messages was "not in [J.K.'s] immediate possession or control," thus entitling J.K. to relief under § 6701. "Immediate" means "[n]ot separated by other persons or things." *Black's Law Dictionary,* p. 816 (9th ed. 2009). The acts complained of occur either after a message is sent or before it is received—but always during transmission,

[23] The California Family Code was created in 1994; this section continues pre-existing law, formerly codified as Civil Code § 33 in 1874 (shortly after the initial adoption of the California's written "Field Codes" in 1872). *See* Civ. Code § 33 (Repealed by Stats.1993, c. 219 (A.B.1500), § 2.)

[24] *See* Cal. Civ. Code § 658, Cal. Civ. Code § 663 ("Every kind of property that is not real is personal.")

[25] "That it is stored in electronic form rather than on ink and paper is immaterial."

and at which time, Gmail users do not have "immediate possession or control" of their email messages. (CC, ¶¶ 22-98.)

Ignoring these allegations, Google asserts without citation that "Plaintiff . . . can select what emails to send, which emails to retain, and which to delete." (MTD, 16:15-18.) Rather, Plaintiffs have alleged that Google secretly extracts data from J.K.'s email, and that the extracted metadata is *not* in control of the minor user, even after J.K. deletes the email. (CC, ¶¶ 269-73.) Accordingly, pursuant to California law, because J.K.'s data within Gmail is personal property not within his immediate possession or control, J.K. has no capacity to consent to Google's interception, scanning, and harvesting of his Gmail messages.

ii. COPPA does not preempt § 6701.

Congress enacted the Children's Online Privacy Protection Act ("COPPA") in 1998 to protect against the collection of personal information over the internet from children under the age of 13.[26] 15 U.S.C. §§ 6501-06. COPPA provides that only state laws "inconsistent" with "***an activity or action described in this title*** [COPPA]" are preempted. 15 U.S.C. § 6502(d) (emphasis added). Federal law preempts state law where: (1) the federal statute expressly says so; (2) Congress preempts the entire field of law; or, (3) the state and federal laws require conflicting or inconsistent compliance. *See Arizona v. United States*, 132 S. Ct. 2492, 2500-01 (2012). There is a presumption against preemption "unless that [is] the clear and manifest purpose of Congress." *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040, 1060 (9th Cir. 2009)(internal citations omitted). Here there is no express, field, or conflict preemption of § 6701.

(a). COPPA Does Not Expressly Preempt § 6701.

By its own terms, COPPA only preempts state laws affecting conduct "described in" COPPA, i.e., the collection of ***personal information*** from children ***under the age of 13***. 15 U.S.C. § 6501(1). Activities of website operators involving persons ***13 years and older*** are not

[26] COPPA defines a "child" as "an individual under the age of 13." 15 U.S.C. § 6501(1).

regulated by, or even mentioned in, COPPA. In fact, because Google does not make Gmail available to anyone under the age of 13, COPPA does not apply to Gmail users, such as J.K.[27,28]

Moreover, COPPA is limited to the collection of *personal information*, and does not expressly abrogate state contract laws, such as § 6701, that void certain contracts by minors. Finally, Google cites no case to support the proposition it now offers—federal preemption of a state law where Congress *could* have regulated the subject but chose not to do so. (MTD, 17.)

(b). COPPA Does Not Preempt The Entire Field Of Law.

The Ninth Circuit has ruled that, as here, a provision stating that "inconsistent" state laws are preempted "unambiguously signifies that Congress did ***not*** intend to occupy the entire field" and "explicitly left room for state . . . authorities to supplement that . . . regulation." *Whistler Invs., Inc. v. Depository Trust & Clearing Corp*., 539 F.3d 1159, 1165 (9th Cir. 2008)(emphasis added).[29]

Field preemption thus is found only where "Congress 'so thoroughly occupies a legislative field,' that it effectively leaves no room for states to regulate conduct in that field." *Whistler Invs., Inc.*, 539 F. 3d at 1164 (quoting *Cipollone v. Liggett Group, Inc.*, 505 U.S. 504, 516 (1992)). Here, the collection of "personal information" (as defined by § 6501(8)) from children under the age of 13 is not the same field of law as the interception of J.K.'s Gmail or the ability of J.K. to make contracts relating to personal property (data amounting to the "substance, purport, or meaning") not in his immediate possession.

(c). Compliance With § 6701 Does Not Conflict With COPPA.

"Conflict preemption analysis examines the federal statute as a whole to determine whether a party's compliance with both federal and state requirements is impossible or whether,

---

[27] Here, Plaintiff J.K. is 16 years old. (CC, ¶ 247.) As alleged in the underlying *A.K.* Complaint (Doc. 45-5, Def. Exhibit EE, ¶ 9), only persons 13 years or older may obtain a Gmail account.

[28] COPPA is a regulatory scheme that governs how Google must conduct itself when its activities involve persons under 13 years. COPPA is not a license to steal from all children older than 12.

[29] *See also Gordon*, 575 F.3d at 1060 ("[The] presumption against preemption leads us to the principle that express preemption statutory provisions should be given narrow interpretation.")(quoting *Air Conditioning & Refrigeration Inst. v. Energy Res. Conservation & Dev. Comm'n*, 410 F.3d 492, 496 (9th Cir. 2005)).

in light of the federal statute's purpose and intended effects, state law poses an obstacle to the accomplishment of Congress's objectives." *Whistler Invs., Inc.,* 539 F.3d at 1164, *citing Crosby v. Nat'l Foreign Trade Council,* 530 U.S. 363, 373 (2000). Here, it is possible for Google to comply with both COPPA and § 6701 simply by obtaining parental consent before: (1) collecting personal information from children under 13 years old (COPPA); and, (2) attempting to contract with minors prior to intercepting their Gmail (§ 6701). *See, e.g.*, *Wyeth v. Levine*, 555 U.S. 555, 573 (2009) (explaining that "[i]mpossibility pre-emption is a demanding defense" and finding no preemption where the defendant could "unilaterally" do what state law required).

Furthermore, § 6701 is not an obstacle to Congress's objectives in COPPA, which is designed to enhance parental involvement in the online activities of children, protect the privacy of children, and prohibit unfair or deceptive practices in connection with the collection, use, or disclosure of children's personal information.[30] Congress's objectives in COPPA did not include the elimination of state contract law protections available to minors not covered by the statute, such as J.K.

In enacting COPPA, Congress chose only to regulate activity involving persons under the age of 13. COPPA contains no regulation concerning persons over the age of 12 (whether minors or adults). Accordingly, there is simply no basis for Google's insistence that COPPA preempts state law restrictions affecting the capacity of minors over the age of 12—restrictions which have existed nearly as long as California has had a written legal code.

3. Although All Google Apps Users Are Conscripted, Google's Terms Still Do Not Provide Consent For Its Actions

As with regular Gmail users, Google secretly extracts, acquires and uses the private and confidential email content of each Google Apps Class Member to create "thought data" and user profiles. The fact that Google intercepts Apps users' email content, despite that it is forbidden by contract to serve advertising, demonstrates that Google's content extraction and acquisition is not for the benefit of its users, but for Google. Plaintiffs do not contend that these allegations

[30] *See* 144 Cong. Rec. S11657 (Daily ed., Oct. 7 1998) (statement of Rep. Bryan); Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999); Sasha Grandison, *The Child Online Privacy Protection Act: The Relationship Between Constitutional Rights and the Protection of Children,* 14 U.D.C. L. Rev. 209, 221 (2011).

undermine the operative agreements between Google, the Apps Customers (contracting party), and the end users (Plaintiffs); Plaintiffs instead allege that Google violates its own agreements with end users and Google Apps Customers through its secret content extraction and acquisition. (*See* Complaint, ¶¶ 102-36 (TOS and Gmail Legal Notice), ¶¶ 137-60 (Cable One's Agreements and Google Apps TOS), ¶¶ 161-83 (Google Apps EDU Agreements and TOS) and ¶¶ 185-97 (Privacy Policy).)

4. Google Is Not A Party To Any Communication, Google Is Not An Agent Of The Recipient, And No Person (Gmail or Non-Gmail) Is Aware Of Its Unlawful Conduct

One cannot consent to what one does not know. Google invites this Court to find that if a person has a basic understanding of email and uses any email service, that person consents to *any and all* interceptions of their email data—even when that person's email servicer performs surreptitious acts of data extraction that are unique in the email service industry and hidden from the public. Google asks this Court to run afoul of every case that has examined the nature of consent—and ECPA's basic purposes. (*See* Section IV B., *supra.*)

Google is neither a party to the communications at issue nor an agent for Gmail senders or recipients. (CC, ¶¶ 292, 327, 335, 348, 369.) Google's disclosures contain no language for such a party or agency theory. Further, Google's attempt to interject a Fourth Amendment privacy issue with its citation to *Smith v. Maryland*, 442 U.S. 735 (1979) is not helpful because Congress overruled *Smith* by enacting 18 U.S.C. §3121(a).

Google also argues that non-Gmail users necessarily give implied consent to Google's secret extraction of the content of their private communications. (MTD, 19-20.) Google asserts, without support, that the "automated processing" of email is so widely understood and accepted that the act of sending an email constitutes implied consent to any and all processing of their emails, regardless of the nature.[31] However, Plaintiffs' claims, including those of non-Gmail users, are not premised on the basic delivery and storage of their emails—Plaintiffs

[31] Google also takes "liberties" with the facts of Plaintiffs' complaint, including inserting un-alleged facts about Plaintiff Fread's state of mind, and the state of mind of non-Gmail Plaintiffs. (MTD, 20:11-16.) Google also ignores the non-Gmail Plaintiffs' allegations that Google extracts the meaning of their communications wholly separate and apart from the automated processes necessary for any person to send and receive email.

allege that Google uses specific devices to extract the *content* of their communication in a process that is distinct from and unnecessary to the reliable delivery of email. Admittedly, phone companies must route telephone calls and transmit them over telephone wires—but no one expects the phone company to decipher their calls, turn them into data, and use the data for any commercial purpose like Google does with email. Likewise, email service providers must direct emails to their recipients, store them on servers, and make them available for viewing. But, it is a violation of ECPA for a non-party to a communication to extract and use the content of the communication without consent. Regardless, it is improper for a court to decide whether Google has established the affirmative defense of consent on a motion to dismiss. *Watkins*, 704 F.2d at 582 ("It is the task of the trier of fact to determine the scope of consent[.]").

5. The California, Florida, Pennsylvania and Maryland Statutes Require All Parties to Consent.

Under California, Florida, Maryland and Pennsylvania's ECPA analogues, the consent defense is only viable where ***all*** parties to the communication consent *in fact* to the alleged interception.[32] Google concedes that the non-Gmail plaintiffs did not expressly consent to Google's interceptions. (MTD, 19:2-5.); *see also* CC, ¶¶ 210-11. In support of implied consent, Google argues that non-Gmail Plaintiffs "must necessarily expect that the communication will be subject to [Google's] systems." (MTD. at 19:12-13.) But Google can't replace Plaintiffs' facts—that no non-Gmail user (including Plaintiffs) has any knowledge or expectation of Google's secret interception, content extraction, acquisition, and use that would support a finding of implied consent. *See* CC, ¶¶ 210-13 and102-209.[33]

///

[32] *See* Cal. Pen. Code §§ 631-32; Florida Statute § 934.03; Md. Code Ann. §10-402; 18 Pa.C.S. §5704.

[33] Google's reliance upon *Commonwealth v. Proetto*, 771 A.2d 823 (Pa. Super. 2001), is misplaced. In *Proetto*, a law enforcement detective, while posing as a 15 year old girl, was the intended recipient of the criminal defendant's communications, and the court determined on review of a suppression motion that "an e-mail… by… [its] nature… can be downloaded, printed, saved [and] the sender expressly consents… to the recording of the message" by the recipient. *Proetto*, at 833. Here, Google is *not* an intended recipient of or party to plaintiffs' emails (CC, ¶¶ 292, 297, 314-15, 327, 335, 348, and 369); Plaintiff's claims are based on the facts that Google (a third-party to the communications) secretly intercepts those communications, extracts the content, and uses that content without Plaintiffs' knowledge or consent. *Proetto* is not helpful to Google.

C. Plaintiffs' CIPA Claims Are Viable

The California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630, *et seq*., provides civil remedies (§ 637.2) for conduct generally referred to as wiretapping (§ 631), and the recording of confidential communications (§ 632). Google's primary argument is that CIPA does not prohibit non-consensual interception, recording, or use of personal email content despite CIPA's broad legislative intent to prevent the invasion of privacy from advances in technology beyond telephone and telegraph mediums of communication:

> The Legislature hereby declares that ***advances in science and technology have led to the development of new devices and techniques*** for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society. The Legislature by this chapter intends to protect the right of privacy of the people of this state. [Cal. Penal Code § 630.] (emphasis added)

1. CIPA Applies To Any "Message" Or "Communication"

The three clauses of § 631 prohibit "three distinct and mutually independent patterns of conduct." *Tavernetti*, 22 Cal. 3d at 192-93. The second clause of § 631, at issue here, provides for a cause of action against "Any person . . . who willfully and without the consent of all parties to the communication, or in an unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state." Google seeks to constrain the application of the second independent clause to only telephone or telegraph communications.[34] However, the first clause of § 631 does not limit the *type of communication*; it prohibits unauthorized connections to certain *types of facilities or systems*—identified as telegraph or telephone. Next, the mutually independent second clause specifically addresses a *medium of communication* ("any message, report, or communication")

[34] Notably, Google adopts the Second Circuit's expansion of ECPA's § 2510(5)(a)(ii) analysis to include ISP equipment when that section only states "telephone" or "telegraph," and yet in the face of *Hall's* interpretation that Congress envisioned advances in technology, Google asserts that the California Legislature intentionally withheld that foresight. *See* MTD 8:16-22; *see also* 18 U.S.C. 2510(5)(a)(ii) definition of device mentioning only "telephone" and "telegraph" as mediums; *and Hall*, 396 F.3d at 505 (finding that although ECPA was enacted in 1986, Congress was aware that electronic communications travelled *over telephone wires*, and, therefore, Congress's use of "'telephone' was thus understood to include the instruments, equipment and facilities that ISPs use to transmit e-mail.").

without limitation to telegraph or telephone.[35] Finally, the ending language of § 631, "or is being sent from, or received at any place within this state," is intended to apply to other unlawful acts, not just those occurring on wires, lines, and cables. And, modern courts have had no problem applying CIPA to electronic communications.[36]

Similarly, § 632 cannot be limited to "oral communications," because it specifically applies to communications carried on "by means of a *telegraph,* telephone, *or other device, except a radio*[.]" Using a telegraph would not entail "oral communications" and the legislature placed no limitation on the *medium* of communication—except by radio.[37]

Next Google completely fabricates the ruling in *Diamond v. Google, Inc.* upon which it relies. *Compare* MTD, 22:6-7 ("[A] California court has specifically held that CIPA does not apply to automated processing of emails in the Gmail system") *with Diamond* Order, Doc. 45-12, Ex. LL to Wong Dec. The *Diamond* court ***did not*** sanction Google's content extraction and acquisition practices or preclude §§ 631's or 632's application to email messages. Instead, the court interpreted § 631 to require email to have "some connection" to a "telegraph or telephone wire, line, cable, or instrument" and further required Plaintiff to plead sufficient facts confirming "Google's 'recording' of [email] communications." (S*ee Diamond* Order, Doc. 45-12, Ex. LL to Wong Dec.) While Plaintiffs disagree with the *Diamond* court's interpretation, Plaintiffs in this case expressly alleged facts that satisfy the *Diamond* ruling. (*See* CC, ¶¶ 305-06.) Moreover, Google has already admitted *in this case* that telegraph is the modern form of email and "Google's automated scanning technology also could be included as 'telegraph equipment.'"[38] Google's basis for such an admission is simple, "telegraphy" is a means for

[35] The Legislature could have very easily used the phrase "telegraph or telephone message, report, or communication," and completely eliminated the necessity for the remainder of the section dealing with how the communication was transmitted—"over any wire, line, or cable."

[36] See *Valentine v. Nebuad*, 804 F.Supp. 2d 1022 (N.D. Cal. 2011) (Applying CIPA to tracking of plaintiffs' web browsing habits); *Bradley v. Google*, 2006 WL 3798134 at *5-6 (N.D. Cal. 2006) (Refusing application of CIPA because plaintiff "has not alleged that Google intercepted her communications, only that her stored emails were deleted.")

[37] "Radio" would not need to be excluded if § 632 was limited to just telephone and telegraph.

[38] *See* Response in Opposition to Motion for Preliminary Injunction, P. 6, [Doc. 36] and Reply to Motion to Dismiss Plaintiff's First Amended Class Action Complaint, P. 1 n.1, [Doc. 48], *Dunbar, et al. v. Google*, 5:10cv194, In The United States District Court for the Eastern District of Texas, Texarkana Division.

"transmitting messages or communications by means of electric currents and signals[.]" *Davis v. Pacific Tel. & Tel. Co.*, 127 Cal. 312, 317 (Cal. 1899). The common meaning of "email" is "a means or system for transmitting messages electronically." www.merriam-webster.com/dictionary/email. As such, email and telegraph are functional equivalents under CIPA. But, Google advocates for a "wooden construction" which is at direct odds with CIPA's express purpose, and California's rules of statutory construction. *Apple, Inc. v. Superior Court*, 56 Cal.4th 128, 138 (Cal. 2013) ("[S]tatutory interpretation must be prepared to accommodate technological innovation, if the technology is otherwise consistent with the statutory scheme.")

Google's argument relating to CIPA's subsequent legislative history specifically ignores that Cal. Penal Code §§ 629, *et seq*. is a separate Penal Code chapter involving police power protections. Google also ascribes unwarranted importance to a hypothetical question posed in a committee analysis document dealing specifically with amendments to the Lawful Interception Act, not CIPA.[39] The *Diamond* court rejected these same arguments already. *Diamond* Order, Doc. 45-12, at 1 ("The legislative history of former Penal Code section 629 does not prove the reach of Penal Code sections 631 or 632 – which are part of a different Penal Code chapter."). The Legislature chose not amend §§ 631 and 632 because no such amendment was necessary—the sections apply to email communications.

2. Plaintiffs Have Standing To Assert CIPA Claims

Section 630 sets forth the injury or harm at issue: an "invasion of privacy" which amounts to "a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Plaintiffs have pleaded: (1) an injury in fact, including Google's statutory violations giving rise to Plaintiffs' causes of action; that (2) is traceable to Google's challenged conduct. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). Furthermore, Plaintiffs seek injunctive relief and request statutory damages under CIPA, Cal

[39] "Although resort to legislative committee reports is appropriate when the meaning of a statute is unclear, the actual language of a statute bears far more significance than statements of legislative committee members." *Guillen v. Schwarzenegger*, 147 Cal.App.4th 929, 947 (Cal. App. Ct. 2007). This is particularly the case where, as here, the hypothetical question relied upon appears in a report involving a different chapter of the Penal Code. See *Santa Clara Local Transportation Authority v. Guardino*, 11 Cal.4th 220, 238 (Cal. App. Ct. 1994)("While an opinion of the Legislative Counsel is entitled to respect, its weight depends on the reasons given in its support.")

Penal Code § 637.2, meaning Plaintiffs' claims are also "redressable." And, Plaintiffs have pleaded a "case or controversy" that gives Plaintiffs Constitutional standing. *See id.*

a. A CIPA violation is an "injury" for purposes of standing.

Google's content extraction and acquisition practices are unlike the "use of Flash cookies to track internet activity." (MTD, 24:17-18.) The Complaint details the evasive privacy violations Google performs on Plaintiffs' emails and the harm envisioned by § 630. "[T]he Supreme Court instructs that a concrete 'injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing.'" *Jewel v. NSA*, 673 F.3d 902, 908 (9th Cir. 2011)(quoting *Lujan*, 504 U.S. at 578).[40] Like ECPA, CIPA prohibits "interception of communications absent compliance with statutory procedures," and "explicitly creates a private right of action for claims of illegal surveillance." *Jewel*, 673 F.3d at 908; *see* Cal. Penal Code § 637.2 ("Any person who has been injured by a violation of this chapter may bring an action against the person who committed the violation . . . (c) ***It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages.***")(emphasis added.) Because CIPA does not require actual damages as a prerequisite for successfully litigating a claim, there is no requirement that a Plaintiff plead actual damages.[41]

b. Plaintiffs have pleaded a particularized grievance.

CIPA Plaintiffs "have alleged such a personal stake in the outcome of the controversy as to warrant . . . invocation of federal-court jurisdiction." *Jewel*, 673 F.3d at 909, *quoting Summers v. Earth Island Inst*., 555 U.S. 488, 493 (2009). Here, Plaintiffs alleged more than Google's general practices and large scale violations of CIPA—Plaintiffs have alleged that they were personally injured by Google's invasion of their privacy. *See id.* at 910 ("Significantly, Jewel alleged with particularity that *her* communications were part of the dragnet.")(emphasis in original). Plaintiffs Scott and Harrington allege that Google's business practices result in the

[40] *See also Low v. LinkedIn Corp*., 900 F. Supp. 2d 1010, 1020-21 (N.D. Cal. 2012).

[41] *See also Ion Equipment Corp. v. Nelson*, 110 Cal. App. 3d 868, 882 (Cal. App. Ct. 1980)("Therefore, even if appellant did not sufficiently allege actual damages, as respondents argued below, it would be entitled to a minimum judgment of $3,000, as actual damages are not a necessary prerequisite to an action pursuant to section 637.2.").

unlawful reading and recording of their email message content. (CC, ¶¶ 287-321.) "[T]he fact that a harm is widely shared does not necessarily render it a generalized grievance." *Jewel*, 673 F.3d at 908. Plaintiffs have pleaded that their own personal emails were intercepted, and the violation of their privacy is a particularized grievance that may be remedied by this Court.

3. The *Scott I* Plaintiffs Allege a California Connection

Paragraph 290 of the Consolidated Complaint, which Google ignores, adequately alleges a California connection to the *Scott I* CIPA claims. (See also *infra* E.3.) Further, § 631's application is not solely limited to messages sent or received in California as Google contends.[42]

D. Section 632 Claims Are Viable

1. Plaintiffs Sufficiently Allege Emails are Confidential Communications

The court in *Diamond* already rejected Google's argument, and rightfully so.[43] Whether a communication is "confidential" has nothing to do with the "content of the conversation." *Flanagan v. Flanagan*, 41 P.3d 575, 581-82 (Cal. 2002). Section 632(c) defines a confidential communication when the circumstances "reasonably indicate that *any* party to the communication desires it to be *confined to the parties thereto*[.]" (Emphasis added.) The focus is on "simultaneous dissemination, not secondhand repetition" to "an unannounced second auditor." *Flanagan*, 41 P.3d at 580. Plaintiffs' email messages are confined to the specified senders and recipients and contain specific "destination address fields" pursuant to defined "Internet Message Formats." (*See* CC, ¶¶ 295-97.) This restriction of the "destination address fields" and the defined parties to the communication "reasonably indicates" the desire that the message be confined to the sender and receiver.

The recording at issue in this case does not involve the placement of the original message into the user's inbox. The allegations of Google's interceptions of Plaintiffs' communications sufficiently detail the surreptitious and "simultaneous dissemination to an

[42] Google chooses to limit § 631's application to this last phrase while completely disregarding the language when applied to the distinction from "wire, line, or cable" discussed *supra.*

[43] *Diamond* Order, Doc. 45-12, at 1. ("Factual questions of whether the senders of email to Gmail recipients impliedly consented' to Google's alleged review [] or have an objectively reasonable expectation[] of confidentiality within the meaning of *Flanagan v. Flanagan*, 27 Cal.4th 766, 768 (2002) . . . cannot be resolved on demurrer[.]").

unannounced second auditor, whether that auditor be a person or a mechanical device." *See Flanagan*, 41 P.3d at 581.[44] Google, not Plaintiffs, fails to address a single detail of its surreptitious activities and separate recordings.

2. ECPA Does Not Preempt CIPA

The *Diamond* court also rejected this argument.[45] The express legislative history of ECPA shows that Congress did not intend for ECPA to preempt state privacy laws.[46] Google argues that ECPA preempts CIPA, and cites *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148 (C.D. Cal. 2006) and *In re Google Inc. Street View Elec. Communs. Litig.*, 794 F. Supp. 2d 1067 (N.D. Cal. 2011). *Bunnell* relies on *Quon v. Arch Wireless Operating Co., Inc.*, 445 F. Supp. 2d 1116 at 1134, 1138 (C.D. Cal. 2006). *Google Street View* relies on *Bunnell*. *Google Street View*, 794 F. Supp. 2d at 1085. All turn on the Stored Communications Act [Title II of ECPA], and none involve the interception of messages prohibited in Title I of ECPA.

Like many others, the court in *Shively v. Carrier IQ, Inc.*, considered ECPA's rich and explicit legislative history, in finding that ". . . *Bunnell* is fundamentally flawed because it fails to take into account the legislative history above. Nor does it account for the language and context of § 2518(10)(c)." 2012 U.S. Dist. LEXIS 103237, at *14. Likewise, the court in *Leong v. Carrier IQ, Inc.*, reached the same conclusion, criticizing *Bunnell's* preemption finding by way of 18 U.S.C. § 2518(10)(c), in these terms: "[i]n this Court's view, that provision does not even impact the question of preemption, but rather focuses on the scope of available

[44] *See also*, *e.g.* CC, ¶¶ 47 (acquisition of message content), 49 (PHIL calculation of actual ideas), 56 (COB's collection of "thought data"), 58, and 102-213 (detailing the secrecy of the actions).

[45] *Diamond* Order, Doc. 45-12, at 2 (". . . Google has not shown that privacy claims involving emails would be preempted by federal law.").

[46] *See* Doc. 51-3, Tapley Exhibit B, Senate Hearing 99-1006, November 18, 1985, page 38 ("It is also true that States would be free to enact more restrictive laws in the area if they so choose. So, to that extent, States are unaffected."); *see also* Doc. 51-4, Tapley Exhibit C, S. Rep. 90-1097, S. Rep. No. 1097, 90th Con., 2nd Sess. 1968, 1968 U.S.C.C.A.N. 2112, 2196 (stating on three occasions, "There is no intent to preempt State Law.").

federal remedies when a violation of the statute has been established. Other courts agree…." *Leong*, 2012 U.S. Dist. LEXIS 59480, at *10.[47]

The *Leong* court added to its criticism of *Bunnell* with its observations of Google's only other preemption authority, *Google Street View*, finding that:

> the analysis in these cases ignores the great weight of authority holding that one of the principal purposes of the federal statute was to establish minimum standards with which states must comply. In that regard, *Bunnell* and *In re Google Inc. Street View* reflect a marked departure from the preemption analysis of courts in this and other districts and circuits in the more than four decades since the Federal Wiretap Act was enacted. In light of the clarity of the 1968 and 1986 Senate Reports that the federal law is intended to establish minimum standards and not to preempt state laws that meet these standards; the long-standing view of the States and courts that States are free to enact legislation that is more restrictive than the federal law; and the rarity with which preemption applies . . . . the Court concludes that the Federal Wiretap Act does not completely preempt California's Invasion of Privacy Act.

Leong, 2012 U.S. Dist. LEXIS 59480 at * 12-13. A two-party consent statute is more restrictive and more protective than ECPA's single-party statute. Likewise, § 632 does not contain the definitional limitations (*e.g.* devices) affording greater protection to users. Multiple courts have rejected Google's assertion of preemption over state privacy laws.[48]

E. Choice-Of-Law Dictates CIPA's Application In This Case

The only choice-of-law analysis currently before this Court is whether the *Scott I* Plaintiffs have adequately pleaded a connection to California under CIPA. (MTD, 27:12-14.)

---

[47] To the extent Google relies upon § 2518(10)(c), every court that has examined the legislative history has rejected any express preemption argument based upon this section—including *In re Google St. View*.

[48] *See Stuart Diamond v. Google, Inc.*, CV1202715, in the Superior Court of California, County of Marin (Doc. 45-2, Tapley Exhibit A); *Debra L. Marquis v. Google, Inc.*, No. 11-2808-BLS1, in the Superior Court of Suffolk County, Commonwealth of Massachusetts (Doc. 45-5, Tapley Exhibit D); *Lane v. CBS Broad, Inc.*, 612 F. Supp. 2d 623 (E.D. Pa. 2009); *Valentine v. Nebuad, Inc.*, 804 F. Supp. 2d 1022 (N.D. Cal. 2011); *Ideal Aeorosmith, Inc. v. Acutronic USA, Inc.*, 87 U.S.P.Q. 2d (BNA) 1756 (W.D. Pa. 2008); *Bansal v. Russ*, 513 F. Supp. 2d 264 (E.D. Penn. 2007); and *In re NSA Telecomms. Records Order Litigation*, 483 F. Supp. 2d 934 (N.D. Cal. 2007). Prior to the 1986 enactment of ECPA, many courts ruled that the preceding Wiretap act did not preempt state law, Congress's intent was to only establish *minimum* standards, and more restrictive state standards were not preempted: *See United States v. Smith*, 726 F.2d 852, 859 (1st Cir. 1984); *State v. Politte*, 664 P.2d 661, 671 (Ariz. App. 1982); *Navarra v. Bache Halsey Stuart Shields, Inc.*, 510 F. Supp. 831 (E.D. Mich. 1981); *State v. Williams*, 617 P.2d 1012, 1017 (Wash. 1980); *State v. Hanley*, 605 P.2d 1087, 1090 (Mont. 1979); *United States v. Testa*, 548 F.2d 847, 856 (9th Cir. 1977); *United States v. Hall*, 543 F.2d 1229, 1232 (9th Cir. 1976); *Commonwealth v. Vitello,* 327 N.W. 2d 819 (Mass. 1975); and *People v. Jones*, 30 Cal. App. 3d 852, 855 (Cal. App. 1973).

See Mazza v. Am. Honda Motor Co., 666 F.3d 581, 590 (9th Cir. 2012)(outlining California's governmental interest analysis for the choice of law).

1. Google's Choice-of-Law argument is premature.

"In a putative class action, the Court will not conduct a detailed choice-of-law analysis during the pleading stage." *In re Sony Grand WEGA KDF-E A10/A20 Series Rear Projection HDTV TV Litig.*, 758 F. Supp. 2d 1077, 1096 (S.D. Cal. 2010). Google's attempt to eliminate Plaintiffs' CIPA claims through a choice-of-law analysis is premature because discovery is necessary to confirm Plaintiffs' allegations in ¶ 290 which, if true, require the application of California law. "Importantly, *Mazza* (and nearly every other case cited by Defendants) undertook a class-wide choice-of-law analysis at the class certification stage, rather than the pleading stage. Until the Parties have explored the facts in this case, it would be premature to speculate about whether the differences in various states' [] laws are material in this case." *Forcellati v. Hyland's, Inc*., 876 F. Supp. 2d 1155, 1159 (C.D. Cal. 2012).

2. Plaintiffs Properly Pleaded Separate and Alternative Legal Theories.

The Court, not the Parties, determines the choice of law that governs Google's unlawful conduct, a determination that is premature at this stage in discovery. Despite Google's urging, this Court should not force Plaintiffs in the underlying, consolidated actions to agree on a single choice-of-law at the pleading stage. A consolidated complaint is not a substantive pleading as Google contends—it is a procedural device for consolidation of the related actions until trial.[49] The Plaintiffs in the underlying actions are entitled to argue choice-of-law after the benefit of discovery. Furthermore, at the pleading stage, even a single Plaintiff in a single underlying action may assert claims in the alternative under the laws of different states.[50] Google also fails

[49] *See, e.g.*, *In re Toyota Motor Corp. Unintended Acceleration Mktg., Sales Practices, & Prods. Liab. Litig.*, 785 F. Supp. 2d 925, 931 (C.D. Cal. 2011)("Neither the general authorization of the coordination and consolidation under the MDL statute nor the more specific use of consolidated complaints, as the Court has required here, is intended to alter the substantive rights of the parties. The use of a consolidated complaint has been described as 'a procedural device rather than a substantive pleading with the power to alter the choice of laws rules applicable to the plaintiffs' claims.' The device does not alter choice-of-law rules[.]")(internal citations omitted).

[50] *See Donohue v. Apple, Inc.*, 871 F. Supp. 2d 913, 923 (N.D. Cal. 2012)("At this stage in the litigation—before the parties have submitted briefing regarding either choice-of-law or class certification—plaintiff is permitted to assert claims under the laws of different states in the alternative.").

to consider that different underlying actions are subject to different choice-of-law analyses. For a state law claim in a diversity action, a transferee Court applies the law of the transferor forum's choice-of-law rules.[51]

3. California's Choice-of-Law analysis supports application of CIPA.

While it is too early to identify all relevant facts that will affect the ultimate choice-of-law governing the various Plaintiffs' claims, the CIPA Plaintiffs properly pleaded facts that support the application of California law. (*See* CC, ¶ 290.) Google's argument that California's choice-of-law principles preclude the CIPA claims of non-California residents relies on Google's false representation that the "communications at issue have no alleged link to California." (MTD, 29 n. 30.) The actual allegations of the CIPA Plaintiffs include: (1) Google is a resident of Mountain View, California; (2) Google's acts in violation of CIPA occurred in the State of California; (3) Google developed and implemented its unlawful business practices and procedures in the state of California; (4) Google profits from this unlawful conduct in California; and, (5) Google developed, designed, built, and physically placed one or more of its accused devices in California. (*See* CC ¶¶ 17, 290.) Because Plaintiffs establish these sufficient constitutional contacts in support of the application of California law, the burden shifts to Google to demonstrate "that foreign law, rather than California law, should apply to class claims." *See Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 590 (9th Cir. Cal. 2012), *quoting Washington Mutual Bank v. Superior Court*, 24 Cal. 4th 906, 921 (Cal. 2001). Here, Google has not carried its burden.

///

///

///

///

///

///

[51] *See, e.g.*, *Menowitz v. Brown*, 991 F.2d 36, 40 (2d Cir. 1993)("[A] transferee court applies the substantive state law, including choice-of-law rules, of the jurisdiction in which the action was filed.").

Google's assertion that "California has *no interest* in applying CIPA to the claims of non-residents" (MTD, 28, emphasis added) finds its sole support in CIPA's statement of purpose which specifically references California residents. But the Northern District of California has explicitly held the opposite:

> The Court declines to read [CIPA's] statement of purpose as a limitation on standing when both statutes expressly allow an action to be brought by 'any person' or by an 'owner or lessee' without imposing any residency requirements. A legislative purpose that articulates an interest in protecting those within California is not inconsistent with also allowing non-Californians to pursue claims against California residents. ***To conclude otherwise would mean the California Legislature intended to allow California residents to violate the CIPA and the CCCL with impunity with respect to out-of-state individuals and entities, a result this Court declines to reach***.

Valentine v. Nebuad, Inc., 804 F. Supp. 2d 1022, 1028 (N.D. Cal. 2011)(emphasis added).

The Supreme Court of California has opined that "California choice-of-law cases nonetheless continue to recognize that a jurisdiction ordinarily has 'the predominant interest' in regulating conduct that occurs within its borders . . . ." *McCann v. Foster Wheeler LLC*, 48 Cal. 4th 68, 97-99 (Cal. 2010)(internal citations omitted).[52] The CIPA Plaintiffs allege that they have been injured by Google, a California resident, from conduct occurring in California which violates California law. (See CC, ¶¶ 17, 290.) Google contends that Alabama and Maryland would be offended if California protects Alabama and Maryland residents from Google's unlawful conduct. (MTD, 28, 30.) But, Google ignores that the CIPA Plaintiffs allege that Google's unlawful conduct occurred in California, providing the CIPA Plaintiffs the protection of California law. (CC ¶¶ 17, 290.) In effect, Google's proposal would render *California* law meaningless by allowing Google to "violate the CIPA . . . with impunity with respect to out-of-state individuals and entities, a result this Court [should] decline[] to reach." *Valentine v. Nebuad, Inc.*, 804 F. Supp. 2d at 1028.

V. CONCLUSION

Google's motion should be denied.

///

[52] *See also McCann*, at 99 ("California's interest in applying its laws providing a remedy to, or facilitating recovery by, a potential plaintiff in a case in which the defendant's allegedly tortious conduct occurred in another state is less than its interest when the defendant's conduct occurred in California.").

Respectfully submitted,

Dated: July 11, 2013

CORY WATSON CROWDER & DEGARIS, P.C.

By: */s/ F. Jerome Tapley*

F. Jerome Tapley (*Pro Hac Vice*)
Email: jtapley@cwcd.com
2131 Magnolia Avenue
Birmingham, AL 35205
Telephone: (205) 328-2200
Facsimile: (205) 324-7896

WYLY~ROMMEL, PLLC
Sean F. Rommel (*Pro Hac Vice*)
Email: srommel@wylyrommel.com
4004 Texas Boulevard
Texarkana, Texas 75503
Telephone: (903) 334-8646
Facsimile: (903) 334-8645

Plaintiffs' Co-Lead Counsel

CARTER WOLDEN CURTIS, LLP
Kirk J. Wolden (SBN 138902)
Email: kirk@cwclawfirm.com
1111 Exposition Boulevard, Suite 602
Sacramento, California 95815
Telephone: (916) 567-1111
Facsimile: (916) 567-1112

Plaintiffs' Liaison Counsel